Boolean Satisfiability Solvers: Techniques and Extensions

Georg WEISSENBACHER a, Pramod SUBRAMANYAN b and Sharad MALIK b

a Vienna University of Technology
b Princeton University

Abstract. Contemporary satisfiability solvers are the cornerstone of many successful applications in domains such as automated verification and artificial intelligence. The impressive advances of SAT solvers, achieved by clever engineering and sophisticated algorithms, enable us to tackle Boolean Satisfiability (SAT) problem instances with millions of variables – which was previously conceived as a hopeless problem. We provide an introduction to contemporary SAT-solving algorithms, covering the fundamental techniques that made this revolution possible. Further, we present a number of extensions of the SAT problem, such as the enumeration of all satisfying assignments (ALL-SAT) and determining the maximum number of clauses that can be satisfied by an assignment (MAX-SAT). We demonstrate how SAT solvers can be leveraged to solve these problems. We conclude the chapter with an overview of applications of SAT solvers and their extensions in automated verification.

Keywords. Satisfiability solving, Propositional logic, Automated decision procedures

1. Introduction

Boolean Satisfiability (SAT) is the problem of checking if a propositional logic formula can ever evaluate to true. This problem has long enjoyed a special status in computer science. On the theoretical side, it was the first problem to be classified as being NP-complete. NP-complete problems are notorious for being hard to solve; in particular, in the worst case, the computation time of any known solution for a problem in this class increases exponentially with the size of the problem instance. On the practical side, SAT manifests itself in several important application domains such as the design and verification of hardware and software systems, as well as applications in artificial intelligence. Thus, there is strong motivation to develop practically useful SAT solvers.

However, the NP-completeness is cause for pessimism, since it is unlikely that we will be able to scale the solutions to large practical instances. While attempts to develop practically useful SAT solvers have persisted for almost half a century, for the longest time it was a largely academic exercise with little hope of seeing practical use. Fortunately, several relatively recent research developments have enabled us to tackle instances with millions of variables and constraints – enabling SAT solvers to be effectively deployed in practical applications including in the analysis and verification of software systems.
This chapter provides an introduction to contemporary SAT-solving techniques and is organised as follows: Section 2 introduces the syntax and semantics of propositional logic. The remaining chapter is split into three parts: The first part (Section 3) covers the techniques used in modern SAT solvers. Further, it covers basic extensions such as the constructions of unsatisfiability proofs. For instances that are unsatisfiable, the proofs of unsatisfiability have been used to derive an unsatisfiable subset of constraints of the formula, referred to as the UNSAT core. The UNSAT core has seen successful applications in model checking. The second part (Section 4) considers extensions of these solvers that have proved to be useful in analysis and verification. Related to the UNSAT core are the concepts of minimal correction sets and maximally satisfiable subsets. A maximally satisfiable subset of an unsatisfiable instance is a maximal subset of constraints that is satisfiable, and a minimal correction set is a minimal subset of constraints that needs to be dropped to make the formula satisfiable. Section 4 discusses how these concepts are related and covers algorithms to derive them. The third part (Section 5) discusses applications of the techniques presented in the Sections 3 and 4 in the field of automated verification. These applications include automated test case generation, bounded model checking and equivalence checking, and fault localisation. Finally, Appendix A provides a number of exercises and their solutions.

2. Preliminaries

This section establishes the notation and syntax we employ throughout this chapter and the meaning (semantics) that is assigned to it.

2.1. Propositional Logic

Propositional logic is a formalism that enables us to make statements about propositions (or variables). While propositions may have some underlying meaning associated with them (e.g., the implicit meaning of $x_1$ being true may be that “it is raining outside”), we do not concern ourselves with such interpretations, but merely require that each proposition can have exactly one of two truth values (true or false).

2.1.1. Notation

Let $\mathcal{V}$ be a set of $n$ propositional logic variables and let 0 and 1 denote the elements of the Boolean domain $\mathbb{B}$ representing false and true, respectively. Every Boolean function $f : \mathbb{B}^n \rightarrow \mathbb{B}$ can be expressed as a propositional logic formula $F$ in $n$ variables $x_1, \ldots, x_n \in \mathcal{V}$. The syntax of propositional logic formulae is provided in Figure 1.

The interpretation of the logical connectives \{$\neg, +, \cdot, \rightarrow, \leftrightarrow, \oplus$\} is provided in Table 1. We use $\equiv$ to denote logical equivalence. For brevity, we may omit $\cdot$ in conjunctions (e.g., $x_1 \neg x_3$). An assignment $\mathcal{A}$ is a mapping from $\mathcal{V}$ to $\mathbb{B}$, and $\mathcal{A}(x)$ denotes the value that $\mathcal{A}$ assigns to $x$. We call $\mathcal{A}$ a total assignment if $\mathcal{A}$ is a total function. Otherwise, $\mathcal{A}$ is a partial assignment. $\mathcal{A}$ satisfies a formula $F(x_1, \ldots, x_n)$ iff $F(\mathcal{A}(x_1), \ldots, \mathcal{A}(x_n))$ is defined and evaluates to 1 (denoted by $\mathcal{A} \models F$). A formula $F$ is satisfiable iff $\exists \mathcal{A} . \mathcal{A} \models F$, and unsatisfiable (inconsistent, respectively) otherwise. We use $\#_{\mathcal{A}F}$ to denote the number of satisfying total assignments of a formula $F$ and drop the subscript if $F$ is clear from the context. A formula $F$ holds iff $\mathcal{A} \models F$ for all total assignments $\mathcal{A}$. 

We use \( \text{Lit}_V = \{x, \overline{x} \mid x \in V\} \) to denote the set of literals over \( V \), where \( \overline{x} \) is the negation of \( x \). Given a literal \( \ell \in \text{Lit}_V \), we write \( \text{var}(\ell) \) to denote the variable occurring in \( \ell \). A cube over \( V \) is a product of literals \( \ell_1 \ldots \ell_m \) such that \( \ell_i \in \text{Lit}_V \) and \( \text{var}(\ell_i) \neq \text{var}(\ell_j) \) for all \( i, j \in \{1 \ldots m\} \) with \( i \neq j \). We write \( \ell \in q \) to indicate that the literal \( \ell \) occurs in a cube \( q \). Given an assignment \( A \), we use \( q_A \) to denote the cube \( \prod_{i=1}^{n} \ell_i \) where \( \ell_i = x_i \) if \( A(x_i) = 1 \) and \( \ell_i = \overline{x}_i \) otherwise. We say that a cube \( q_i \) covers cube \( q_j \) if every literal in \( q_i \) is also present in \( q_j \). Cubes corresponding to a total assignment are called \textit{minterms}. In the sequel, we use minterms and total assignments as well as cubes and partial assignments interchangeably.

### 2.1.2. Conjunctive Normal Form

The Conjunctive Normal Form (CNF) of a formula is a restricted form of propositional logic formulae. Figure 2 shows the syntax of propositional logic formulae in CNF. A formula in CNF is product of sums (a conjunction of clauses, respectively). Note that the empty clause (denoted by \( \square \)) corresponds to the logical value \( 0 \).

The formula \( \overline{x}_1 \cdot (x_1 + x_2) \cdot (x_1 + x_2) \cdot x_1 \) is in CNF, for instance. A commonly used alternative (and more compact) representation of this formula is \( (\overline{x}_1) (x_1 \overline{x}_2) (\overline{x}_1 x_2) (x_1) \), i.e., the logical connectives \( \cdot \) and \( + \) are dropped, since they are clear from the context.

Clauses are commonly regarded as \textit{sets of literals}. While we stick to the notation defined in Figure 2, we will implicitly assume that clauses have the properties of sets of literals. Accordingly, \( (\overline{x}_1 x_2 x_2) \) and \( (x_1 x_2) \) are indistinguishable from their logically equivalent counterparts \( (\overline{x}_1 x_2) \) and \( (x_2 x_1) \), respectively. Therefore, a formula in CNF is a set of sets of literals. Note that this representation implicitly incorporates \textit{factoring} (i.e., merging of unifiable literals).

### Table 1. Definition of Propositional Logic Operators

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( x \cdot y )</th>
<th>( x + y )</th>
<th>( x \rightarrow y )</th>
<th>( x \leftrightarrow y )</th>
<th>( x \oplus y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

### Figure 1. Syntax of Propositional Logic

\[
\text{formula} ::= \text{formula} \cdot \text{formula} | \text{formula} + \text{formula} \\
\text{formula} \rightarrow \text{formula} | \text{formula} \leftrightarrow \text{formula} \\
\text{formula} \oplus \text{formula} | \text{formula} | (\text{formula}) | \text{atom}
\]

\[
\text{atom} ::= \text{propositional identifier} | \text{constant}
\]

\[
\text{constant} ::= 1 | 0
\]

### Figure 2. Syntax of Propositional Logic in Conjunctive Normal Form

\[
\text{formula} ::= \text{formula} \cdot (\text{clause}) | (\text{clause})
\]

\[
\text{clause} ::= \text{clause} + \text{literal} | \text{literal}
\]

\[
\text{literal} ::= \text{atom} | \text{atom}
\]

\[
\text{atom} ::= \text{propositional identifier}
\]
Each formula $F$ in propositional logic can be transformed into CNF. Unfortunately, the resulting formula may be exponentially larger than $F$. It is, however, possible to construct a formula $G$ in CNF such that $F$ and $G$ are equi-satisfiable (i.e., $(\exists A . A \models F) \leftrightarrow (\exists A . A \models G)$) and the size of $G$ is polynomial in the size of the original formula $F$. Such an equi-satisfiable formula can be obtained by means of Tseitin’s transformation \[Tse83\]. Given a formula $F$ in propositional logic (as defined in Figure 1), this transformation involves the following steps:

1. Recursively replace each sub-formula $(F_1 \vartriangle F_2)$ of the original formula $F$ (where $\vartriangle \in \{-, +, \cdot, \rightarrow, \leftrightarrow, \oplus\}$) with a fresh propositional identifier $x$ and add the constraint $x \leftrightarrow (F_1 \vartriangle F_2)$.
2. Rewrite the resulting formula into CNF by using the rules presented in Table 2.

**Example 2.1** We demonstrate Tseitin’s transformation by converting the formula $(y \leftrightarrow z)$ into conjunctive normal form.

1. The first step is to replace $(y \leftrightarrow z)$ with a fresh propositional identifier $x_1$. After adding the corresponding constraint, we obtain $x_1 \cdot (x_1 \leftrightarrow (y \leftrightarrow z))$.
2. In the next step, we replace $x_1$ with $x_2$. This step is optional, since $(x_1)$ is already in clausal form. This transformation step yields the formula

   \[
   x_2 \cdot (x_2 \leftrightarrow (y \leftrightarrow z)) \cdot (x_1 \leftrightarrow (y \leftrightarrow z)) \cdot (x_1 \leftrightarrow (y \leftrightarrow z)),
   \]

3. This formula can be rewritten according to Table 2:

   \[
   x_2 \cdot (x_2 \leftrightarrow (x_1 \leftrightarrow (y \leftrightarrow z))) \cdot (x_1 \leftrightarrow (y \leftrightarrow z)) \cdot (x_1 + y + z + x_1).
   \]

4. We obtain an equi-satisfiable formula in CNF:

   \[
   x_2 \cdot (x_1 + x_2) \cdot (x_1 + y + z + (x_1 + y + z + x_1)) \cdot (x_1 + y + z + x_1).
   \]

We also encourage the reader to solve the Exercises 1 and 2 in Section A.

3. **Boolean Satisfiability Checking: Techniques**

   In this section, we formally introduce the problem of Boolean satisfiability (SAT) and present a number of techniques to tackle it.

3.1. **Problem Definition**

**Definition 3.1 (Boolean Satisfiability Problem)** Given a propositional logic formula $F$, determine whether $F$ is satisfiable.

The Boolean Satisfiability Problem, usually referred to as SAT, is a prototypical NP-complete problem \[Coo71\], i.e., there is no known algorithm that efficiently solves all instances of SAT. While Definition 3.1 refers to formulae in propositional logic in general, the problem can be easily reduced to formulae in CNF: Using Tseitin’s transforma-
Negation:
\[ x \leftrightarrow y \equiv (x \rightarrow y) \cdot (\neg y \rightarrow x) \equiv (\neg x + y) \cdot (y + x) \]

Disjunction:
\[ x \leftrightarrow (y + z) \equiv (y \rightarrow x) \cdot (z \rightarrow x) \cdot (x \rightarrow (y + z)) \equiv (\neg y + x) \cdot (\neg z + x) \cdot (\neg x + y + z) \]

Conjunction:
\[ x \leftrightarrow (y \cdot z) \equiv (x \rightarrow y) \cdot (x \rightarrow z) \cdot ((y \cdot z) \rightarrow x) \equiv (\neg x + y) \cdot (\neg x + z) \cdot (y + z + x) \]

Equivalence:
\[ x \leftrightarrow (y \leftrightarrow z) \equiv (x \rightarrow (y \leftrightarrow z)) \cdot ((y \leftrightarrow z) \rightarrow x) \equiv (x \rightarrow ((y \rightarrow z) \cdot (z \rightarrow y)) \cdot ((y \leftrightarrow z) \rightarrow x) \equiv (\neg x + y) \cdot (\neg x + z) \cdot ((y \cdot z) \rightarrow x) \equiv (\neg x + y) \cdot (\neg x + z) \cdot (y + z + x) \cdot (y + z + x) \]

Equivalence (c.f. Section 2.1.2), any arbitrary propositional formula can be transformed into an equi-satisfiable formula in clausal form. It is therefore sufficient to focus on formulae in CNF.

There are two important sub-classes of SAT:

- **2-SAT**: Each clause of the formula contains at most 2 literals. The satisfiability of such 2-CNF formulae can be decided in polynomial time [Kro67]: each clause \((\ell_1 \ell_2)\) can be rewritten as an implication \(\ell_1 \rightarrow \ell_2\) (or \(1 \rightarrow \ell_1\) and \(\ell_1 \rightarrow 0\) in case of a clause \((\ell_1)\) with only one literal). The formula is satisfiable if the transitive closure of the implications does not yield 0. This approach effectively amounts to resolution (see Section 3.2).

- **3-SAT**: Each clause of the formula contains at most 3 literals. This form is relevant because any arbitrary formula in CNF can be reduced to an equi-satisfiable 3-CNF formula by means of Tseitin’s transformation (Section 2.1.2).

### 3.2. Resolution Proofs

The *resolution principle* states that an assignment satisfying the clauses \(C + x\) and \(D + \neg x\) also satisfies \(C + D\). The clauses \(C + x\) and \(D + \neg x\) are the *antecedents*, \(x\) is the *pivot*, and \(C + D\) is the *resolvent*. Let \(\text{Res}(C, D, x)\) denote the resolvent of the clauses \(C\) and \(D\).

---

**Table 2.** Tseitin transformation [Tse83] for standard Boolean connectives
$D$ with the pivot $x$. The corresponding resolution rule is formally described below.

$$
\frac{C + x}{C + D} \quad \frac{D + \overline{x}}{[\text{Res}]}
$$

Resolution corresponds to existential quantification of the pivot and subsequent quantifier elimination, as demonstrated by the following sequence of logical transformation steps (where $F(x \leftarrow e)$ denotes the substitution of all free occurrences of $x$ in $F$ with the expression $e$):

$$
\exists x . (C + x) \cdot (D + \overline{x})
\equiv (((C + x) \cdot (D + \overline{x}))_{(x \leftarrow 1)} + ((C + x) \cdot (D + \overline{x}))_{(x \leftarrow 0)})
\equiv (C + 1) \cdot (D + 1) + (C + 0) \cdot (D + 0)
\equiv C + D
$$

The repeated application of the resolution rule results in a resolution proof.

**Definition 3.2** A resolution proof $R$ is a directed acyclic graph $(V_R, E_R, \text{piv}_R, \lambda_R, s_R)$, where $V_R$ is a set of vertices, $E_R$ is a set of edges, $\text{piv}_R$ is a pivot function, $\lambda_R$ is the clause function, and $s_R \in V_R$ is the sink vertex. An initial vertex has in-degree 0. All other vertices are internal and have in-degree 2. The sink has out-degree 0. The pivot function maps internal vertices to pivot variables of the respective resolution step. For each internal vertex $v$ and $(v_1, v), (v_2, v) \in E_R$, $\lambda_R(v) = \text{Res}(\lambda_R(v_1), \lambda_R(v_2), \text{piv}_R(v))$.

A resolution proof $R$ is a refutation if $\lambda_R(s_R) = \Box$. A refutation $R$ is a refutation for a formula $F$ (in CNF) if the label of each initial vertex of $R$ is a clause of $F$.

**Example 3.1 (Unit Propagation and Resolution)** Figure 3 shows an example of a resolution proof for the formula

$$
(\overline{x}_1) \cdot (x_1 + \overline{x}_2) \cdot (x_1 + x_2) \cdot (x_1).
\quad (3.1)
$$

In Figure 3, each node $v$ is represented by its label $\lambda(v)$ (the parentheses around the literals are dropped since each node is associated with exactly one clause and there is no risk of ambiguity). Moreover, Figure 3 does not show the pivot variables explicitly, since they are uniquely determined by the clauses labelling a node and its predecessors and therefore clear from the context.

Note that this formula is a 2-CNF formula and can therefore be solved by means of transitive closure of the corresponding implications. Equivalently, the unsatisfiability of Formula (3.1) can be established by repeated application of the unit-resolution rule:

$$
\ell \quad \frac{D + \overline{\ell}}{D} \quad [\text{URes}]
$$

Here, $\ell$ denotes a literal over the pivot variable.
3.3. The Davis-Putnam Procedure

The resolution rule is sufficient to devise a complete algorithm for deciding the satisfiability of a CNF formula [Rob65].

**Theorem 3.1 (Completeness of Propositional Resolution)** If $F$ is an inconsistent formula in CNF, then there is a resolution refutation for $F$.

**Proof sketch.** By induction over the number of variables in $F$ (c.f. [Bus98]). In the base case, where no variables appear in $F$, the formula must contain the empty clause $\square$. For the induction step, let $x$ be a fixed variable in $F$, and let $F_1$ to be the formula defined as follows:

1. For all clauses $(C + x)$ and $(D + \neg x)$ in $F$, the resolvent $\text{Res}((C + x), (D + \neg x), x)$ is in $F_1$.
2. Every clause $C$ in $F$ which contains neither $x$ nor $\neg x$ is in $F_1$.

It is clear that $x$ does not occur in $F_1$ unless $F$ contains trivial clauses $C$ for which $\{x, \neg x\} \subseteq C$. W.l.o.g., such tautological clauses can be dropped. Then, $F_1$ is satisfiable if and only if $F$ is, from whence the theorem follows by the induction hypothesis.

**Remark** Resolution is merely refutation-complete, i.e., while it is always possible to derive $\square$ from an inconsistent formula, it does not enable us to derive all valid implications: we cannot deduce $(x + y)$ from $(x)$ by means of resolution, for instance, even though the latter obviously entails the former.

The constructive proof sketch above is interesting for two reasons:

- It demonstrates that propositional resolution is refutation-complete even if we fix the order of pivots along each path in the proof, and
- It outlines a decision procedure which is known as Davis-Putnam procedure [DP60].

We refer to the algorithm presented in [DP60] as “Davis-Putnam” procedure or simply DP. The Davis-Putnam procedure comprises three rules:

1. **1-literal rule.** Whenever one of the clauses in $F$ is a unit clause, i.e., contains only a single literal $\ell$, then we obtain a new formula $F_1$ by

   (a) removing any instances of $\ell$ from the other clauses, and
   (b) removing any clause containing $\ell$, including the unit clause itself.

   This rule obviously subsumes unit-resolution (see Example 3.1).

2. **The affirmative-negative rule.** If any literal $\ell$ occurs only positively or only negatively in $F$, then remove all clauses containing $\ell$. This transformation obviously preserves satisfiability.
3. The rule for eliminating atomic formulae. For all clauses \((C + x)\) and \((D + \overline{x})\) in \(F\), where neither \(C\) nor \(D\) contain \(x\) or \(\overline{x}\), the resolvent \(\text{Res}((C + x), (D + \overline{x}), x)\) is in \(F_1\). Moreover, every clause \(C\) in \(F\) which contains neither \(x\) nor \(\overline{x}\) is in \(F_1\).

The last rule can make the formula increase in size significantly. However, it completely eliminates all occurrences of the atom \(x\). The correctness of the transformation is justified by the resolution principle (see Section 3.2).

In practice, the resolution rule should only be applied after the 1-literal rule and affirmative-negative rule. The 1-literal rule is also known as unit propagation and lends itself to efficient implementations.

Once this option is exhausted, we face a choice of which pivot variable \(x\) to resolve on. While there is no “wrong” choice that forfeits completeness (as established in the proof of Theorem 3.1), a “bad” choice of a pivot may result in a significant blowup of the formula, and therefore retard the performance of the solver. We postpone the discussion of selection strategies to Section 3.7.

3.4. The Davis-Putnam-Logeman-Loveland Procedure

For realistic problems, the number of clauses generated by the DP procedure grows quickly. To avoid this explosion, Davis, Logemann, and Loveland [DLL62] suggested to replace the resolution rule with a case split. This modified algorithm is commonly referred to as DPLL procedure. It is based on the identity known as Shannon’s expansion [Sha49]:

\[ F \equiv x \cdot F(x \leftarrow 1) + \overline{x} \cdot F(x \leftarrow 0) \]  

(3.2)

Accordingly, checking the satisfiability of a formula \(F\) can be reduced to testing \(F \cdot x\) and \(F \cdot \overline{x}\) separately. The subsequent application of unit propagation (the 1-literal rule, respectively) can reduce the size of these formulae significantly. This transformation, applied recursively, yields a complete decision procedure.

In practice, this split is not implemented by means of recursion but in an iterative manner (using tail recursion, respectively). We keep track of the recursive case-splits and their implications using an explicit trail. Each entry in this trail represents an assignment to a variable of \(F\) imposed by either a case split or by unit propagation. We refer to the former kind of entries as guessed and to the latter as implied assignments.

**Definition 3.3 (Clauses under Partial Assignments)** A trail represents a partial assignment \(A\) to the variables \(\mathcal{V}\) of \(F\).

- A clause \(C\) is satisfied if one or more of its literals evaluates to 1 under the partial assignment \(A\).
- A clause \(C\) is conflicting if all of its literals are assigned and \(C\) evaluates to 0 under \(A\).
- A clause \(C\) becomes unit under a partial assignment if all but one of its literals are assigned but \(C\) is not satisfied. As such, \(C\) gives rise to an implied assignment. In this case, we say that \(C\) is the antecedent of the implied assignment.
- In all other cases, we say that the clause \(C\) is unresolved.
Example 3.2 Consider the clauses

\[ C_1 \equiv (\overline{x}_1 \overline{x}_3) \quad \text{and} \quad C_2 \equiv (\overline{x}_3 \overline{x}_2). \]

Table 3 shows a possible trail for this instance. Initially, neither of the clauses is unit, forcing us to guess an assignment for one of the variables and thus to introduce a new decision. We choose to assign \( x_1 \) first. The first entry in the trail, the literal \( x_1 \), represents this decision. Neither of the clauses is unit under this assignment; we decide to assign \( x_4 \). The clause \( C_1 \) is unit under the partial assignment \( \{ x_1 \mapsto 1, x_4 \mapsto 1 \} \) and implies the assignment \( x_3 \mapsto 1 \) (note that we mark the assignment as “implied” in the trail). This assignment, in turn, makes \( C_2 \) unit, imposing the assignment \( x_2 \mapsto 0 \). The resulting assignment satisfies \( C_1 \) as well as \( C_2 \).

A trail may lead to a dead end, i.e., result in a conflicting clause, in which case we have to explore the alternative branch of one of the case splits previously made. This corresponds to reverting one of the decisions or backtracking, respectively.

Example 3.3 (Backtracking) Consider the set of clauses

\[ C_1 \equiv (x_2 \overline{x}_3) \quad C_2 \equiv (\overline{x}_1 \overline{x}_4) \quad C_3 \equiv (\overline{x}_2 x_4) \quad C_4 \equiv (x_1 x_2 x_3). \]

Figure 4(a) shows a trail that leads to a conflict (assignments are represented as literals, c.f. Section 2.1.1). Clause \( C_4 \) is conflicting under the given assignment. The last (and only) guessed assignment on the given trail is \( x_1 \mapsto 1 \). Accordingly, we backtrack to this most recent decision (dropping all implications made after this point) and revert it to \( x_1 \mapsto 0 \) (see Figure 4(b)). We tag the assignment \( x_1 \mapsto 0 \) as implied, since \( x_1 \mapsto 1 \) led to a conflict. Thus, we prevent that this assignment is reverted back to \( x_1 \mapsto 1 \) at a later point in time, which would lead to a non-terminating loop.

When backtracking enough times, the search algorithm always yields a conflicting clause or a satisfying assignment and eventually exhausts all branches. However, always reverting the last decision made is not necessarily the best strategy, as the following example from [Har09] shows.

Example 3.4 Consider the clauses \( C_1 \equiv (\overline{x}_1 x_n x_{n+1}) \) and \( C_2 \equiv (\overline{x}_1 \overline{x}_n x_{n+1}) \) as part of an unsatisfiable formula \( F \). Exploring the trail \( x_1 x_2 \cdots x_{n-1} x_n \) leads to a conflict forcing us to backtrack and explore the trail \( x_1 x_2 \cdots x_{n-1} \overline{x}_n \). Since \( F \) is unsatisfiable, we are eventually (perhaps after further case-splits) forced to backtrack. Unfortunately, each time we change one of the assignments to \( x_2, \ldots, x_{n-1} \), we will unnecessarily explore the case in which \( x_n \) is 1 again, since the solver is “unaware” of the fact that \( x_1 \rightarrow \overline{x}_n \) (which follows from \( \text{Res}(C_1, C_2, x_{n+1}) \)).

<table>
<thead>
<tr>
<th>Level</th>
<th>Partial Assignment</th>
<th>Clauses</th>
<th>Trail</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>–</td>
<td>(\overline{x}_1 \overline{x}_3)(\overline{x}_1 x_2)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>{ x_1 \mapsto 1 }</td>
<td>(\overline{x}_1 \overline{x}_3)(\overline{x}_1 x_2)</td>
<td>( x_1 ), guessed</td>
</tr>
<tr>
<td>2</td>
<td>{ x_1 \mapsto 1, x_4 \mapsto 1 }</td>
<td>(\overline{x}_1 \overline{x}_3)(\overline{x}_3 \overline{x}_2)</td>
<td>( x_4 ), guessed</td>
</tr>
<tr>
<td></td>
<td>{ x_1 \mapsto 1, x_4 \mapsto 1, x_3 \mapsto 1 }</td>
<td>(\overline{x}_3)(\overline{x}_3 \overline{x}_2)</td>
<td>( x_3 ), implied</td>
</tr>
<tr>
<td></td>
<td>{ x_1 \mapsto 1, x_4 \mapsto 1, x_3 \mapsto 1, x_2 \mapsto 0 }</td>
<td>(\overline{x}_2)</td>
<td>( x_2 ), implied</td>
</tr>
</tbody>
</table>

Table 3. Assignment trail for Example 3.2
The next section introduces conflict clauses as a means to prevent the repeated exploration of infeasible assignments.

3.5. Conflict-Driven Clause Learning

In their solvers GRASP and RELSAT, João Marques-Silva and Karen Sakallah [MSS96], and Roberto Bayardo and Robert Schrag [JS97], respectively, introduced a novel mechanism to analyse the conflicts encountered during the search for a satisfying assignment.

First, they partition trails into decision levels according to recursion depth of the case-splits performed.

**Definition 3.4 (Decision Levels)** Each recursive application of the splitting rule gives rise to a new decision level. If a variable $x$ is assigned 1 (owing to either a case split or unit propagation) at decision level $n$, we write $x @ n$. Conversely, $\overline{x} @ n$ denotes an assignment of 0 to $x$ at decision level $n$.

Secondly, the implications in a trail are represented using an implication graph.

**Definition 3.5 (Implication Graph)** An implication graph is a labelled directed acyclic graph $G(V, E)$.

- The nodes $V$ represent assignments to variables. Each $v \in V$ is labelled with a literal and its corresponding decision level.
- Each edge in an implication graph represents an implication deriving from a clause that is unit under the current partial assignment. Edges are labelled with the respective antecedent clauses of the assignment the edge points to.
- An implication graph may contain a single conflict node (indicated by the symbol □), whose incoming edges are labelled with the corresponding conflicting clause.
Figure 5. An implication graph for the trail in Table 3

Figure 6. An implication graph with a conflict

Example 3.5 (Implication Graph for Example 3.2) Figure 5 shows the implication graph for the trail presented in Example 3.2.

If the implication graph contains a conflict, we can use it to determine the decisions that led to this conflict. Moreover, it enables us to derive a conflict clause, which, if added to the original formula, prevents the algorithm from repeating the decision(s) that led to the conflict.

Example 3.6 (Implication Graph with Conflict) Figure 6 shows an implication graph for a trail emanating from the decision \( x_1 \mapsto 1 \) for the clauses

\[
C_1 \equiv (x_2 \land x_3), \quad C_2 \equiv (\neg x_1 \land x_4), \quad C_3 \equiv (x_2 \land \neg x_4), \quad C_4 \equiv (\neg x_1 \land x_2 \land x_3).
\]

The final node in the graph represents a conflict. The initial node of the graph is labelled with the decision that causes the conflict. Adding the unit clause \( (x_1) \) to the original clauses guarantees that the decision \( x_1 \) will never be repeated.

Example 3.7 Figure 7 shows a partial implication graph for the clauses

\[
C_1 \equiv (\neg x_1 \land x_3 \land x_5), \quad C_2 \equiv (\neg x_1 \land x_2), \quad C_3 \equiv (\neg x_2 \land x_4), \quad \text{and} \quad C_4 \equiv (x_3 \land x_4)
\]

and the decisions \( x_1 \oplus 5 \) and \( \neg x_5 \oplus 2 \). Using the implication graph, the decisions responsible for the conflict can be easily determined. Adding the conflict clause \( (x_1 + x_5) \) to the original formula rules out that this very combination of assignments is explored again.

The advantage of conflict clauses over simple backtracking becomes clear when we revisit Example 3.4. Using an implication graph, we can quickly determine the assignments \( x_1 \oplus 1 \) and \( x_n \oplus m \) which caused a conflict for either \( C_1 \equiv (\neg x_1 \land x_n \land x_{n+1}) \) or \( C_2 \equiv (\neg x_1 \land x_n \land \neg x_{n+1}) \). The conflict clause \( (\neg x_1 + x_n) \) eliminates this combination, pruning a large fraction of the search space which simple backtracking would have otherwise explored.

After adding a conflict clause, at least some of the decisions involved in the conflict need to be reverted (otherwise, the trail remains inconsistent with the clauses). Changing an assignment in the trail might invalidate all subsequently made decisions. Therefore, if
we backtrack to a certain decision level $n$, we discard all decisions made at a level higher than $n$. It is clear that, of all decisions contributing to the conflict clause, we have to at least revert the one associated with the current decision level ($x_1 @ 5$ in Example 3.7, for instance). The conflict-driven backtracking strategy suggests to backtrack to the second most recent decision level in the conflict clause [MZX+01] (level 2 in Example 3.7). This strategy has a compelling advantage: The conflict clause is unit or assertive under the resulting partial assignment. For instance, $(\overline{x}_1 + x_5)$ in Example 3.7 immediately implies $x_1$ in this scenario.

### 3.6. Conflict Clauses and Resolution

Clause learning with conflict analysis does not impair the completeness of the search algorithm: even if the learnt clauses are dropped at a later point during the search, the trail guarantees that the solver never repeatedly enters a decision level with the same partial assignment.

We show the correctness of clause learning by demonstrating that each conflict clause is implied by the original formula. The following example is based on [KS08].

**Example 3.8 (Conflict Clauses and Resolution)** Figure 8 shows a partial implication graph for the clauses

\[
C_1 \equiv (\overline{x}_4 x_{10} x_6) \quad C_2 \equiv (\overline{x}_4 x_2 x_5) \quad C_3 \equiv (\overline{x}_5 \overline{x}_6 \overline{x}_7) \quad C_4 \equiv (\overline{x}_6 x_7) .
\]

The conflicting clause in this example is $C_4$. The immediate cause for the conflict are assignments $x_6 @ 6$ and $\overline{x}_7 @ 6$ to the literals $x_6$ and $x_7$ of the clause $C_4$. These literals are implied by the clauses $C_3$ and $C_1$, respectively. Clearly, $C_3$ and $C_4$ (and $C_1$ and $C_4$) do not agree on the assignment of $x_7$ (and $x_6$, respectively). Accordingly, if we construct the resolvent of $C_3$ and $C_4$ for the pivot $x_7$, we obtain a clause $C_5$:

\[
C_5 \equiv \text{Res}(C_4, C_3, x_7) \equiv (\overline{x}_5 \overline{x}_6)
\]
While \( C_5 \) is certainly conflicting under the current partial assignment, we will not use it as a conflict clause: both \( x_5 \) and \( x_6 \) are assigned at decision level 6 and therefore \( C_5 \) is not assertive after backtracking.

As previously mentioned, \( C_1 \) is the antecedent of \( x_6 \), and by a similar resolution step as before we obtain

\[
C_6 \equiv \text{Res}(C_5, C_1, x_6) \equiv (\overline{x}_4 \overline{x}_5 x_{10})
\]

Again, \( x_4 \) as well as \( x_5 \) are assigned at decision level 5. The clause \( C_2 \) is the antecedent of \( x_5 \), and we execute a final resolution step:

\[
C_7 \equiv \text{Res}(C_6, C_2, x_5) \equiv (x_2 \overline{x}_4 x_{10})
\]

The resulting clause \((x_2 \overline{x}_4 x_{10})\) has the virtue of containing only one literal which is assigned at decision level 6 while still conflicting with the current partial assignment. Accordingly, if we backtrack to a decision level below 6, \( C_7 \) becomes assertive, forcing the solver to flip \( x_4 \). Therefore, we choose \( C_7 \) as conflict clause. Note that this clause corresponds to a cut (shown in Figure 8) that separates the (implied and guessed) decisions causing the conflict from the conflicting node.

We observe in Example 3.8 that it is possible to derive a conflict clause from the antecedents in the implication graph by means of resolution. These antecedents might in turn be conflict clauses. However, by induction, each conflict clause is implied by the original formula. Formal arguments establishing the completeness and correctness of clause learning and conflict analysis are provided in [MS95,MS99,Zha03].

The following example (based on the example presented in [MSS96]) demonstrates that, in general, there is a choice of assertive conflict clauses.
Figure 9. An implication graph with two unique implication points

Figure 10. Possible cuts separating decision variables from the conflicting clause

Example 3.9 Consider the partial implication graph in Figure 9. Figure 10 shows three possible cuts that separate the decisions causing the conflict from the conflicting node. This results in three candidates for conflict clauses:

1. $C_7 \equiv (x_8 \bar{x}_1 \bar{x}_7 \bar{x}_9)$
2. $C_8 \equiv (x_8 \bar{x}_4 \bar{x}_9)$
3. $C_9 \equiv (x_8 \bar{x}_2 \bar{x}_3 \bar{x}_9)$
If conflict at decision level 0 → UNSAT
Repeat:
1. If all variables assigned return SAT
2. Make decision
3. Propagate constraints
4. No conflict? Go to 1
5. If decision level = 0 return UNSAT
6. Analyse conflict
7. Add conflict clause
8. Backtrack and go to 1

Figure 11. The DPLL algorithm with clause learning

We can dismiss the last clause, since it fails to be assertive after backtracking. The clauses \((x_8 x_1 x_7 x_9)\) and \((x_8 x_4 x_9)\), however, are viable candidates for a conflict clause.

The distinguishing property of clauses \(C_7\) and \(C_8\) when compared to clause \(C_9\) in Example 3.9 is that the former two clauses contain only one literal assigned at the current decision level. This literal corresponds to a unique implication point (UIP).

Definition 3.6 (Unique Implication Point) A unique implication point is any node (other than the conflict node) in the partial conflict graph which is on all paths from the decision node\(^1\) to the conflict node of the current decision level.

Accordingly, we can stop searching for a conflict clause (which is done by means of resolution) once we reach a unique implication point. But which UIP should we choose? We will base our choice on the following property of the conflict clause corresponding to the UIP closest to the conflict (referred to as the first UIP): by construction, the conflict clause induced by the first UIP subsumes any other conflict clause except for the asserting literal. For instance, in Example 3.9, \(C_7 \equiv (x_8 \overline{x}_1 x_7 x_9)\) contains all literals that occur in \(C_8 \equiv (x_8 x_4 x_9)\), except for the literal \(x_4\) which was assigned at decision level 6. Therefore, choosing \(C_8\) as conflict clause has the following advantages:

1. The conflict clause \(C_8\) is smaller than \(C_7\), making it a more likely candidate for unit implications at a later point in the search algorithm.
2. Stopping at the first UIP has the lowest computational cost.
3. The second most recent decision level in the clause \(C_8\) is at least as low as in any other conflict clause, which forces the solver to backtrack to a lower decision level.

The “first UIP” strategy is implemented in CHAFF [ZMMM01], whereas GRASP [MSS96], in contrast, learns clauses at all UIPs.

Figure 11 shows the complete DPLL algorithm with clause learning.

\(^1\)The decision node of the current decision level is a unique implication point by definition.
3.7. Decisions and Decision Heuristics

Step 2 of the algorithm Figure 11 leaves the question of which variable to assign open. As we know from Section 3.3, this choice has no impact on the completeness of the search algorithm. It has, however, a significant impact on the performance of the solver, since this choice is instrumental in pruning the search space.

3.7.1. 2 Literal Watching for Unit Propagation

The choice is clear as long as there are clauses that are unit under the current assignment. The book-keeping required to detect when a clause becomes unit can involve a high computational overhead if implemented naïvely, though. The authors of the CHAFF solver [MZM+01] observed that it is sufficient to watch in each clause any two literals that have not been assigned, yet: a clause with \( m \) literals can only be unit (or conflicting) after at least \( m - 1 \) of its literals have been set to 0. Assignments to the non-watched literals can be safely ignored. When a variable is assigned 1, the solver only needs to visit clauses where the corresponding watched literal is negated. Each time one of the watched literals is assigned 0 the solver chooses one of the remaining unassigned literals to watch. If this is not possible, the clause is necessarily unit under the current partial assignment: any sequence of assignments that makes a clause unit will include an assignment of one of the watched literals. The computational overhead of this strategy is relatively low: in a formula with \( n \) clauses and \( m \) variables, \( 2 \cdot n \) literals need to be watched, and \( n/m \) clauses are visited per assignment on average. One of the key advantages of this approach is that the watched literals do not need to be updated upon backtracking. This is in contrast to the solver SATO [Zha97], for instance, which uses head and tail pointers that need to be updated whenever decisions are reverted.

In the case that no clauses are unit under the current partial assignment, however, it is necessary to choose a decision variable in step 2 in Figure 11. In the following, we will discuss only a few such selection strategies; we refer the reader to [MS99] and [KS08] for a more complete overview over heuristics for choosing decision variables.

3.7.2. Dynamic Largest Individual Sum

It is conventional wisdom that it is advantageous to assign the most tightly constrained variables, i.e., variables that occur in a large number of clauses. On representative of such a selection strategy is known as the dynamic largest individual sum (DLIS) heuristic. At each decision point, it chooses the assignment that satisfies the most unsatisfied clauses. Formally, let \( p_x \) be the number of unresolved clauses containing \( x \) and \( n_x \) be the number of unresolved clauses containing \( \overline{x} \). Moreover, let \( x \) be variable for which \( p_x \) is maximal, and let \( y \) be variable for which \( n_y \) is maximal. If \( p_x > n_y \), choose 1 as the value for \( x \). Otherwise, choose \( y \rightarrow 0 \). The disadvantage of this strategy is that the computational overhead is high: the algorithm needs to visit all clauses that contain a literal that has been set to true in order to update the values \( p_x \) and \( n_x \) for all variables contained in these clauses. Moreover, the process needs to be reversed upon backtracking.

3.7.3. Variable State Independent Decaying Sum

A heuristic commonly used in contemporary SAT solvers favours literals in recently added conflict clauses. Each literal is associated with a counter, which is initialised to
zero. Whenever a (conflict) clause is added, its literals are *boosted*, i.e., the respective counters are increased. Periodically, all counters divided by constant, resulting in a decay causing a bias towards recent conflicts. At each decision point, the solver then chooses the unassigned literal with the highest counter (where ties are broken randomly by default). This approach, known as the *variable state independent decaying sum* (VSIDS) heuristics, was first implemented in the CHAFF solver [MZM+01]. CHAFF maintains a list of unassigned literals sorted by counter. This list is only updated when conflict clauses are added, resulting in a very low overhead. Decisions can be made in constant time.

The emphasis on variables that are involved in recent conflicts leads to a *locality* based search, effectively focusing on sub-spaces [MZ09]. The sub-spaces induced by this decision strategy tend to coalesce, resulting in more opportunities for resolution of conflict clauses, since most of the variables are common.

Representing the counter using integer variables leads to a large number of ties. MINISAT avoids this problem by using a floating point number to represent the weight [?]. Another possible (but significantly more complex) strategy is to concentrate only on unresolved conflicts by maintaining a stack of conflict clauses [GN02].

### 3.8. Unsatisfiable Cores

Given an unsatisfiable instance \( F \), we can use the techniques described in Section 3.6 to construct a resolution refutation (see Definition 3.2 in Section 3.2). Intuitively, such a refutation identifies a *reason* for the inconsistency of the clauses in \( F \). The clauses at the leaves of a resolution refutation are a subset of the clauses of \( F \). By construction, the conjunction of these clauses is unsatisfiable.

**Definition 3.7 (Unsatisfiable Core)** Given an unsatisfiable formula \( F \equiv C_1 \cdot C_2 \cdots C_n \), any unsatisfiable subset of the set of clauses of \( F \) is an unsatisfiable core.

Resolution proofs and unsatisfiable cores have applications in hardware verification [McM03]. Note that a formula typically does not have a unique unsatisfiable core. The following example demonstrates how we can use a SAT solver to construct an unsatisfiable core.

**Example 3.10 (Constructing Unsatisfiable Cores)** Consider the following formula in conjunctive normal form:

\[
(\overline{x} + y) \cdot (\overline{x} + \overline{y}) \cdot (x + z) \cdot (x + \overline{x}) \cdot (z + y + \overline{x})
\]

The problem instance does not contain unit literals, so the satisfiability solver is forced to make a decision. The VSIDS heuristic (see Section 3.7) assigns the highest priority to the literal \( \overline{x} \). Accordingly, the solver assigns \( x \rightarrow 0 \). This decision immediately yields a conflict, as depicted in Figure 12(a). Accordingly, the solver derives a conflict clause \( (\overline{x}) \) – the justifying resolution step is shown in Figure 12(b). The conflict clause \( (\overline{x}) \) forces the solver to assign \( x \rightarrow 1 \) at decision level zero \( (x@0) \). Again, this leads to a conflict (see Figure 12(c)). The corresponding conflict clause is \( (\overline{x}) \) (see Figure 12(d)). This time, however, the conflict occurs at decision level zero and the satisfiability solver
determines that the instance is unsatisfiable. The SAT solver finalises the resolution proof by resolving \((\overline{\tau})\) and \((\tau)\) (see Figure 12(e)).

The unsatisfiable core

\[
\{ \ (\overline{\tau} + y), \ (\overline{\tau} + \overline{y}), \ (x + z), \ (x + \overline{z}) \ \}
\]

can be easily extracted from the resolution proof in Figure 12(e). The clause \((z + y + \overline{\tau})\) did not contribute to the contradiction and is therefore not contained in the core.

An unsatisfiable core is minimal if removing any clause from the core makes the remaining set of clauses satisfiable.

**Definition 3.8 (Minimal and Minimum Unsatisfiable Cores)** Let \(UC\) be an unsatisfiable core of the formula \(F\) (i.e., a set of clauses \(UC \subseteq F\) such that \(C_1 \cdot C_2 \cdots C_n \rightarrow 0\) if \(C_i \in UC\) for \(1 \leq i \leq n\)). The unsatisfiable core \(UC\) is minimal if removing any one of its clauses \(C_i\) leaves the conjunction of the remaining clauses \(UC \setminus C_i\) satisfiable. An unsatisfiable core is minimum if the original formula does not contain an unsatisfiable core \(UC_2\) such that \(|UC_2| < |UC|\).

3.9. Incremental Satisfiability Solving

Many applications of SAT solvers require solving a sequence of similar instances which share a large number of clauses. Incremental satisfiability solvers [Str01,KSW01] support the reuse of learnt clauses in subsequent calls to the SAT solver when only a fraction of the clauses of the original problem have changed. To this end, an incremental solver drops all learnt clauses and reverts all decisions that derive from clauses that are part of the original instance but not of the subsequent related problem.
Example 3.11 Recall the formula from Example 3.3:

\[(x_1 + x_3) \cdot (\overline{x}_1 + x_4) \cdot (\overline{x}_2 + x_4) \cdot (\overline{x}_1 + x_2 + \overline{x}_3)\]

Assume that the SAT solver derives the initial satisfying assignment

\[\{x_1 \mapsto 0, x_2 \mapsto 0, x_3 \mapsto 1, x_4 \mapsto 0\}\]

for this formula, which can be represented as the cube \(\overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \cdot \overline{x}_4\). Note that at this point the SAT solver has learnt the clause \((\overline{x}_1)\) (c.f. Figure 4).

Assume that in the next step we want to add the clause \((x_1 + x_2 + \overline{x}_3 + x_4)\) (which happens to be the negation of \(x_1 \cdot x_2 \cdot x_3 \cdot x_4\)) to the current set of clauses:

\[
(x_2 + x_3) \cdot (\overline{x}_1 + x_4) \cdot (\overline{x}_2 + x_4) \cdot (\overline{x}_1 + x_2 + \overline{x}_3) \cdot (\overline{x}_1 + x_2 + \overline{x}_3 + x_4)\]

Note that, while we have to revert the decisions made during the first run of the SAT solver, we are allowed to retain the learnt clause \((\overline{x}_1)\), since it is a logical consequence of the original formula (i.e., at decision level 0). The SAT solver can now proceed to find a new satisfying assignment (e.g., \(\{x_1 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 1, x_4 \mapsto 1\}\)). In this example, the new clause \((x_1 + x_2 + \overline{x}_3 + x_4)\) guarantees that this assignment differs from the previous one.

3.10. Pre-processing Formulae

This section covers pre-processing techniques presented in [EB05] which enable us to reduce the size of the formula either before passing it to a satisfiability checker or during the search process.

3.10.1. Subsumption

A clause \(C_1\) is said to subsume a clause \(C_2\) if \(C_1 \subseteq C_2\), i.e., all literals in \(C_1\) also occur in \(C_2\). If formula in CNF contains two clauses \(C_1\) and \(C_2\) such that \(C_1\) subsumes \(C_2\), then \(C_2\) can be discarded. This is justified by the fact that, given a resolution proof, we can replace any occurrence of a clause \(C_2\) by a clause \(C_1\) which subsumes \(C_2\) without invalidating the correctness of the proof. In fact, such a modification typically enables a reduction of the size of the proof [BIFH+11].

3.10.2. Self-subsuming Resolution

Even though initial instance does not necessarily contain clauses subsuming others, such clauses may materialise during the search process. Eén and Biere [EB05] observes that formulae in CNF often contain clauses \((x + C_1)\) which almost subsume clauses \((\overline{x} + C_2)\) (where \(C_1 \subseteq C_2\)). After one resolution step we obtain the clause \(\text{Res}(x + C_1, \overline{x} + C_2) = C_2\), which subsumes \((\overline{x} + C_2)\). Accordingly, the clause \((\overline{x} + C_2)\) can be dropped after resolution. Eén and Biere dubbed this simplification rule self-subsuming resolution.

Efficient data structures for implementing (self-)subsumption are presented in [EB05].
3.10.3. Variable Elimination by Substitution

Formulae that are encoded in CNF using the transformation introduced in Section 2.1.2 (or a similar approach) typically contain a large number of functionally dependent variables, namely the fresh variables introduced to represent terms (or gate outputs, respectively). In the following formula, for instance, the value of the variable \( x \) is completely determined by the values of \( y \) and \( z \) (c.f. Example 2.1):

\[
(x \leftrightarrow (y \leftrightarrow z)) \quad (\overline{x} + \overline{y} + z) \quad (\overline{x} + x + y) \quad (\overline{y} + \overline{x} + z) \quad (y + z + x)
\]

The algorithms previously presented are oblivious to this structural property and therefore fail to exploit it. Één and Biere [EB05] presents an approach that eliminates dependent variables by substitution in an attempt to reduce the size of the resulting formula. First, note that the auxiliary variable \( x \) can be eliminated using the rule for eliminating atomic formulae introduced in Section 3.3. The application of this rule amounts to variable elimination by means of resolution. In general, given a set \( S \) of clauses all of which contain \( x \), we can partition \( S \) into clauses containing \( x \) and clauses containing \( \overline{x} \). Let \( S_x \triangleq \{ C \mid C \in S, x \in C \} \) and \( S_{\overline{x}} \triangleq \{ C \mid C \in S, \overline{x} \in C \} \). Abusing the notation we introduced in Section 3.2, we define

\[
\text{Res}(S_x, S_{\overline{x}}, x) \triangleq \{ \text{Res}(C_x, C_{\overline{x}}, x) \mid C_x \in S_x, C_{\overline{x}} \in S_{\overline{x}} \}.
\]

A clause is trivial if it contains a literal and its negation. We observe that the pairwise resolution of the clauses corresponding to a definition of \( x \) introduced by the Tseitin transformation (see Table 2) yields only trivial clauses. We demonstrate this for the definition \( x \leftrightarrow (y \leftrightarrow z) \) introduced in Example 2.1. Let

\[
G \triangleq \{(\overline{x} + \overline{y} + z), (\overline{x} + x + y), (\overline{y} + \overline{x} + z), (y + z + x)\}
\]

denote the set of clauses introduced by the transformation. Splitting \( G \) as suggested above yields

\[
G_{\overline{x}} = \{(\overline{x} + \overline{y} + z), (\overline{x} + x + y)\} \quad G_x = \{(\overline{y} + \overline{x} + z), (y + z + x)\},
\]

and we obtain

\[
\text{Res}(G_x, G_{\overline{x}}, x) = \{(\overline{y} + z + \overline{x}), (\overline{y} + z + y), (\overline{x} + y + \overline{y}), (\overline{y} + y + \overline{x})\}.
\]

The reader may verify that this holds for all transformations presented in Table 2. Accordingly, given a set of clauses \( S \) (all of which contain \( x \)) and the definition \( G \subseteq S \) of \( x \), we can safely omit the resolution steps \( \text{Res}(G_x, G_{\overline{x}}, x) \). Let \( R = S \setminus G \) be the remaining clauses that are not part of the definition of \( x \). Then one can partition \( \text{Res}(S_x, S_{\overline{x}}, x) \) into

\[
\underbrace{\text{Res}(R_x, G_{\overline{x}}, x)}_{S''} \cdot \underbrace{\text{Res}(G_x, G_{\overline{x}}, x)}_{G'} \cdot \underbrace{\text{Res}(G_x, G_x, x)}_{R'} \cdot \underbrace{\text{Res}(R_x, R_x, x)}_{R''}.
\]
In our example, \( G_x \) and \( G_\forall \) encode \( x + (y \leftrightarrow z) \) (i.e., \( \overline{x} \rightarrow (y \leftrightarrow z) \)) and \( \overline{x} + (y \leftrightarrow z) \), respectively. Accordingly, \( \text{Res}(R_x, G_x, x) \) can be interpreted as substitution of \( (y \leftrightarrow z) \) for \( x \) in \( R_x \) (and similarly for \( \text{Res}(G_x, R_\forall, x) \)). As a consequence, \( R'_x \) can be derived from \( S'' \) in a single hyper-resolution step (or a sequence of resolution steps) [GOMS04]. It is therefore admissible to replace \( S \) with \( S'' \).

**Example 3.12** Consider the CNF instance
\[
(x_1 + u) \cdot (\overline{x}_1 + v) \cdot (\overline{x}_1 + \overline{y} + z) \cdot (\overline{x}_1 + \overline{z} + y) \cdot (\overline{y} + \overline{z} + x_1) \cdot (y + z + x_1). 
\]
We obtain
\[
S'' \equiv (u + \overline{y} + z) \cdot (u + \overline{z} + y) \cdot (v + \overline{y} + \overline{z}) \cdot (v + y + z),
\]
allowing us to reduce the size of the original formula by two clauses.

A more elaborate example for this approach is provided in Exercise 10 in Appendix A.

### 4. Boolean Satisfiability Checking: Extensions

After covering contemporary techniques to generate satisfying assignments or refutation proofs for propositional formulae in Section 3, we address a number of extensions of the SAT problem (Definition 3.1). As we will see, an in-depth understanding of the internals of SAT solvers is crucial to the techniques discussed in this section – na"ively applying a SAT solver as a black box may result in a suboptimal performance of the resulting algorithm.

#### 4.1. All-SAT

Given a satisfiable formula, the algorithms presented in Section 3 provide a single satisfying assignment. Some applications, however, require us to enumerate all satisfying assignments of a formula. This is called the All-SAT problem and has many diverse applications such as model checking [McM02,GGA04], the computation of backbones of a propositional logic formula [ZWSM11,MSJL10], quantifier elimination [BKK11], logic minimization [STC03], reachability analysis [GSY04] and predicate abstraction [LBC03].

**Definition 4.1 (All-SAT Problem)** Given a propositional formula \( F \) in conjunctive normal form, derive a disjunction of cubes \( Q = q_1 + q_2 + \cdots + q_m \), such that \( Q \) is equivalent to \( F \), i.e., \( Q \leftrightarrow F \).

The All-SAT problem is equivalent to that of converting a conjunction of clauses (CNF) to a disjunction of cubes, also known as the disjunctive normal form (DNF).
Algorithm 4.1.1. Naïve All-SAT Algorithm

Input: $F$ in CNF.
Output: $Q$ in DNF, such that $Q \leftrightarrow F$.
1: $i := 1$, $F_1 = F$, $Q = 0$
2: while not unsat($F_i$) do
3: $m_i := \text{sat}(F_i)$ \Comment{get a satisfying assignment of $F_i$}
4: $C_i := \overline{m_i}$ \Comment{compute blocking clause}
5: $Q := Q + m_i$, $F_{i+1} = F_i \cdot C_i$ \Comment{update $Q$ and $F_i$}
6: $i := i + 1$
7: end while
8: return $Q$.

4.1.1. Naïve All-SAT

Algorithm 4.1.1 is a naïve solution for the All-SAT problem. Line 3 uses the SAT solver to identify a single minterm that satisfies the formula $F_i$. Lines 4 and 5 derive a blocking clause $C_i$ and append it to the formula $F_{i+1}$. The blocking clause is just the complement of the minterm $m_i$ and prevents $m_i$ from being a solution during a subsequent call to the SAT solver. This process is repeated until each minterm in the formula is enumerated and at this point the formula $F_i$ will be unsatisfiable. The number of satisfying assignments of propositional logic formulas can be exponential in the size of the formula. As a result, this algorithm is likely not practical.

For good performance, it is important in Algorithm 4.1.1, as well as the other All-SAT algorithms in this section, to take advantage of incremental satisfiability checking (c.f. Section 3.9) during the repeated calls to the SAT solver.

4.1.2. All-Clause All-SAT Algorithm

Algorithm 4.1.2. All-Clause Algorithm

Input: $F$ in CNF.
Output: $Q$ in DNF, such that $Q \leftrightarrow F$.
1: $i := 1$, $F_1 = F$, $Q = 0$
2: while not unsat($F_i$) do
3: $m_i := \text{sat}(F_i)$ \Comment{get a satisfying assignment (minterm) of $F_i$}
4: $(q_i, C_i) := \text{minimal}(m_i, F_i)$ \Comment{get cube and blocking clause using from minterm}$
5: $Q := Q + q_i$, $F_{i+1} = F_i \cdot C_i$ \Comment{update $Q$ and $F_i$}
6: $i := i + 1$
7: end while
8: return $Q$.

A more efficient template for the All-SAT problem was introduced by McMillian [McM02]. The key insight is to enlarge the total assignment obtained from the SAT solver into a partial assignment. Each partial assignment consists of a set of total assignments and the blocking clause added to the formula blocks all the total assignments contained in the partial assignment. The set of partial assignments may be enumerable in practice even if the set of total assignments is not, so this algorithm may successfully complete on instances that the naïve algorithm is unable to handle.
The process described above is shown in Algorithm 4.1.2 and following the terminology from [YSTM14], we shall refer to this as the All-Clause algorithm. Line 3 uses the SAT solver to compute a satisfying minterm \( m_i \). The minterm \( m_i \) is enlarged into a cube/partial assignment \( q_i \) in line 4 by calling the \textit{minimal} function. \textit{minimal} also returns the blocking clause \( C_i \) corresponding to \( q_i \). The cube \( q_i \) is added to the solution and the blocking clause \( C_i \) is appended to \( F_{i+1} \) to prevent any minterm in \( q_i \) from being enumerated in subsequent iterations. This process is depicted pictorially in Figure 13(a).

4.1.3. Finding Minimal Blocking Clauses

The \textit{minimal} function takes as input a minterm \( m_{sat} \) and a formula \( F \) and returns the "enlarged" cube \( q_i \) and corresponding blocking clause \( C_i \). In other words, given the minterm \( m_{sat} \), the goal here is to identify a subset of the literals in \( m_{sat} \) which guarantee satisfiability of \( F \). This is the unate covering or hitting set problem. Precisely stated, the problem is to select a subset of columns that cover every row of a matrix \( A_{m \times n} \). Here each of the \( m \) rows corresponds to a clause in \( F \) while each column corresponds to a literal in the minterm \( m_{sat} \). \( A_{ij} = 1 \) if the \( j \)-th literal in \( m_{sat} \) occurs in clause \( C_i \), and 0 otherwise. Column \( j \) is said to cover row \( i \) iff \( A_{ij} = 1 \).

The unate covering problem can be solved using a greedy heuristic [HS96]. First select all essential columns. A column \( j \) is essential if there is at least one row \( i \) such that \( A_{ij} = 1 \) and \( A_{ik} = 0 \) for all \( k \neq j \). Essential columns and rows covered by them are eliminated from the matrix. Next dominated rows are pruned. Row \( i \) is dominated by row \( j \) if \( \forall k : A_{jk} = 1 \rightarrow A_{ik} = 1 \). Column \( i \) is dominated by column \( j \) if \( \forall k : A_{ki} = 1 \rightarrow A_{kj} = 1 \). Dominated columns are also pruned. These pruning techniques are applied repeatedly until no new rows/columns can be eliminated. At this point, a column that covers the most rows is greedily selected, this column and the rows covered by it are removed, and the above procedure is repeated until all rows are covered. The conjunction of the selected columns (i.e., literals in \( m_{sat} \)) yields \( q_i \) and its negation is the disjunction \( C_i \), the blocking clause. It is worth noting that minimal satisfying cubes correspond to \textit{prime implicants} [HS96] of \( F \).

![Figure 13. Difference between All-Clause and Non-Disjoint Algorithms.](image-url)
4.1.4. Non-Disjoint All-SAT Algorithm

An important observation about the All-Clause algorithm is the cubes derived by it are pairwise disjoint.

**Theorem 4.1 (Disjoint Cubes)** Let \( Q = q_1 + q_2 + \cdots + q_k \) be the disjunction of cubes produced by Algorithm 4.1.2. \( \forall i, j \in \{1 \ldots k\} : (i \neq j) \rightarrow (q_i \cdot q_j = 0) \).

*Proof Sketch.* The function \( \text{minimal} \) takes an input a minterm \( m_{sat} \) and a function \( F \) and returns a cube \( q_i \) which is an “enlargement” of \( q_i \) and the blocking clause \( C_i \) which is the complement of \( q_i \). In Algorithm 4.1.2, \( m_{sat} = m_i \) and \( F = F_i \). Note \( F_i \) contains the blocking clauses \( C_1, C_2, \ldots, C_{i-1} \). All minterms in \( q_i \) must satisfy these clauses, which means \( q_i \) cannot contain minterm also contained in \( q_1, q_2, \ldots, q_{i-1} \).

Counting the number of satisfying assignments of a formula is \( \#P \)-complete [GSS08, AB09]. However, this can be computed in polynomial time given a set of pairwise disjoint cubes, as the disjoint cube property ensures no satisfying minterm is counted twice. However, most problems related to computing a minimal DNF cover are in \( \Sigma^P_2 \) [BU11], so it is likely that determining a DNF representation is simpler than model counting. This suggests the All-Clause algorithm is doing more work than necessary.

Using the above insight, the Non-Disjoint All-SAT Algorithm [YSTM14] computes a disjunction of overlapping cubes \( Q \) with the expectation that \( Q \) would be more compact. This is shown in Algorithm 4.1.3. In line 4, \( \text{minimal} \) enlarges the minterm \( m_i \) into a cube \( q_i \) that satisfies \( F \) but not necessarily \( F_i \). Figure 13(b) shows this pictorially: cubes \( q_1, q_2, q_3 \) etc. can now overlap with the other cubes. The DNF representation \( Q \) can no longer be used to count the number of satisfying assignments in polynomial time and thus its generation is not obviously \( \#P \)-complete.

**Algorithm 4.1.3. Non-Disjoint Algorithm**

```
Input: \( F \) in CNF.
Output: \( Q \) in DNF, such that \( Q \leftrightarrow F \).
1: \( i := 1 \), \( F_1 = F \), \( Q = 0 \)
2: \textbf{while not} \( \text{unsat}(F_i) \) \textbf{do}
3: \( m_i := \text{sat}(F_i) \) \hfill \( \triangleright \) get a satisfying assignment (minterm) of \( F_i \)
4: \( (q_i, C_i) := \text{minimal}(m_i, F) \) \hfill \( \triangleright \) get cube and blocking clause from minterm
5: \( Q := Q + q_i \), \( F_{i+1} = F_i \cdot C_i \) \hfill \( \triangleright \) update \( Q \) and \( F_i \)
6: \( i := i + 1 \)
7: \textbf{end while}
8: \textbf{return} \( Q \).
```

The Non-Disjoint algorithm was introduced in [YSTM14].

4.1.5. Example: All-Clause and Non-Disjoint Algorithms

Consider \( F = (a + \overline{b}) \cdot (a + b + c) \). This function has five satisfying minterms and two minimal satisfying cubes (prime implicants): \( q_1 = \overline{b} \cdot c \), \( q_2 = a \). The naïve algorithm will enumerate all five minterms of \( F \). Table 4 shows one possible execution of the All-Clause algorithm for the same function. Execution starts by finding the minterm \((a \cdot \overline{b} \cdot c)\). This minterm can be expanded to the cube \((\overline{b} \cdot c)\) but blocking this cube now means that
Table 4. Example: Execution of All-Clause Algorithm for $F = (a + b) \cdot (a + b + c)$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$m_i$</th>
<th>$q_i$</th>
<th>$C_i$</th>
<th>$F_{i+1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a \cdot b \cdot c$</td>
<td>$b \cdot c$</td>
<td>$b + \tau$</td>
<td>$F \cdot (b + \tau)$</td>
</tr>
<tr>
<td>2</td>
<td>$a \cdot b \cdot \tau$</td>
<td>$a \cdot \tau$</td>
<td>$\pi + c$</td>
<td>$F \cdot (b + \tau) \cdot (\pi + c)$</td>
</tr>
<tr>
<td>3</td>
<td>$a \cdot b \cdot c$</td>
<td>$a \cdot b \cdot c$</td>
<td>$\pi + b + \tau$</td>
<td>$F \cdot (b + \tau) \cdot (\pi + c) \cdot (\pi + b + \tau)$</td>
</tr>
</tbody>
</table>

Table 5. Example: Execution of Non-Disjoint Algorithm for $F = (a + b) \cdot (a + b + c)$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$m_i$</th>
<th>$q_i$</th>
<th>$C_i$</th>
<th>$F_{i+1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a \cdot \pi$</td>
<td>$b \cdot c$</td>
<td>$b + \tau$</td>
<td>$F \cdot (b + \tau)$</td>
</tr>
<tr>
<td>2</td>
<td>$a \cdot b \cdot \tau$</td>
<td>$a \cdot \tau$</td>
<td>$\pi$</td>
<td>$F \cdot (b + \tau) \cdot (\pi)$</td>
</tr>
</tbody>
</table>

cube $q_2 = a$ cannot be found as $a$ alone does not satisfy the blocking clause $(b + \tau)$. The result of the All-Clause procedure is a disjunction of three pairwise disjoint cubes.

Table 5 shows the execution of the Non-Disjoint algorithm for the same function and the same initial minterm. In this case, the ability to select overlapping cubes results in a more compact (and in fact optimal) DNF representation.

4.2. Backbones of a Satisfiable Formula

The backbones of a satisfiable formula consist of the set of variables in formula which take the same constant value of either 0 or 1 in all satisfying assignments to the formula. Backbones are also known as fixed variables and their applications include post-silicon debug [ZWM11] and solutions to the Max-SAT problem [ZRL03,MB05].

The term backbone was coined by researchers investigating the hardness of instances of NP-complete problems [MZK+99,AGKS00,KRA01,CG01,Zha01,Zha04]. The backbone represents the strongly constrained variables of a SAT instance and its size is one parameter studied in this context.

**Definition 4.2 Fixed Variable**

*Given a satisfiable formula $F$ over $\mathcal{V}$, a variable $x_i \in \mathcal{V}$ is fixed in $F$ if either $A(x_i) = 1$ for all $A \models F$ or $A(x_i) = 0$ for all $A \models F$, i.e., if either $(F \rightarrow x_i)$ or $(F \rightarrow \neg x_i)$ holds.*

Our goal is to determine the set $\mathcal{F} \subseteq \mathcal{V}$ of all fixed variables for $F$. We assume that $F$ is a satisfiable formula over $\mathcal{V}$, else $\mathcal{F} = \emptyset$ holds trivially. In the formula

$$F = (x_1 \oplus x_2 \oplus x_3) \wedge (x_1 \oplus x_2),$$  \hspace{1cm} (4.1)

for instance, $x_3$ is fixed to 1, while $x_1$ and $x_2$ are not fixed.

A number of quite sophisticated algorithms to identify fixed variables/backbones have been proposed [MSJL10,ZWM11,KK01]. Experimental evidence [ZWM11] suggests that probing is most effective in practice.

4.2.1. Identifying Backbones Through Probing

Given an initial satisfying assignment $A \models F$, the set $\mathcal{F}$ can be determined by solving $n$ independent SAT instances. In each of these instances, we constrain one variable $x$ in $F$
to take the value opposing \( A(x) \). The variable \( x \) is fixed iff \( F \cdot (A(x) \oplus x) \) is unsatisfiable. Algorithm 4.2.1 computes the set \( F \) by probing each variable independently.

**Algorithm 4.2.1. Identifying Backbones Through Probing and Recording**

**Input:** \( F \) in CNF where \( F \) is over \( V \).

**Output:** \( F \): Subset of the variables in \( V \) that are backbones.

```
1: \( F := \emptyset \), \( N := \emptyset \)
2: for all \( l \in q_A \) do
3: \( P := V \setminus (N \cup F) \)
4: if \( \text{var}(l) \in P \) then \( \triangleright \) Only consider potentially fixed variables.
5: if \( \not\exists A' \mid (F \cdot \overline{l}) \) then \( \triangleright \) No satisfying assignments when \( l \) is forced to \( \overline{l} \)?
6: \( F := F \cup \{\text{var}(l)\} \)
7: \( N := \text{RECORD}(A, A', F, N) \)
8: end if
9: end for
10: procedure \( \text{RECORD}(A, A', F, N) \)
11: for all \( x \in (V \setminus (N \cup F)) \) do
12: if \( (A(x) \neq A'(x)) \) then \( \triangleright \) Does the assignment to \( x \) differ between \( A \) and \( A' \)?
13: \( N := N \cup \{x\} \)
14: end if
15: end for
16: return \( N \)
17: end procedure
```

Contemporary SAT solvers support repeated incremental calls with differing assumptions (e.g., \( \overline{l} \)) about \( V \) in the form of cubes [ES04], which performs significantly better than restarts. The solver only discards the information inferred from \( \overline{l} \) and retains the learnt clauses derived from \( F \). This is crucial to the feasibility of probing [ZWM11].

Note that each iteration of line 6 potentially provides us with a new satisfying assignment \( A' \mid (F \cdot \overline{l}) \). By construction, \( A' \) disagrees with \( A \) on the value of at least one variable. The assignments \( A \) and \( A' \), however, may differ in more than just one variable. The discrepancy between \( A \) and \( A' \) can be used to derive an (initially empty) set \( N \) of variables that are definitely not fixed. The discrepancy between \( A \) and \( A' \) can be used to derive an (initially empty) set \( N \) of variables that are definitely not fixed. This technique is called **recording** and is shown in the procedure \( \text{RECORD} \) in Algorithm 4.2.1. Recording can rapidly reduce the number of potentially fixed variables \( P = V \setminus (N \cup F) \).

Consider the example of Formula (4.1). Suppose \( A = \{x_1 \mapsto 0, x_2 \mapsto 0, x_3 \mapsto 1\} \). Let us probe the variable \( x_1 \) first. This will find the satisfying assignment \( A' = \{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1\} \). This means that \( x_1 \) is not a backbone because the satisfying assignment \( A' \) exists. Furthermore, recording also tells us that \( x_2 \) is not a backbone because its value differs between \( A \) and \( A' \).

Probing requires \( n = |V| \) iterations (each of which involves a call to the SAT solver) in the worst case, but may terminate after \( |F| \) (or \( n - |N| \), respectively) iterations in the best case if paired with recording (where \( F \) and \( N \) represent to the final results of the algorithm).

Probing as well as recording were introduced in [KK01].
4.3. Cardinality Constraints

Satisfiability solvers are designed to work in the Boolean domain and do not support numeric reasoning per se. There is a number of applications for which it is desirable, however, to have at least rudimentary support for arithmetic over bounded domains. A common approach is to represent binary numbers using the two’s complement system and to encode arithmetic operations using their corresponding circuit representation. Figure 14 shows the encoding of addition/subtraction as a ripple-carry-adder (Figure 14(a)), implemented as a chain of full adders (Figure 14(b)). This technique is known as eager bit-flattening. We refer the reader to [KS08] for a more detailed treatment of this topic.

Cardinality constraints are a common application of numerical constraints. Given a set \( \{ \ell_1, \ldots, \ell_n \} \) of literals, a cardinality constraint \( (\sum_i \ell_i) \leq k \) rules out all assignments in which more than \( k \) of these literals evaluate to 1 (here, \( \sum \) denotes the arithmetic sum and not the logical “or” operator). This constraint can technically be encoded by constructing a circuit that computes \( k - (\sum_i \ell_i) \) (using a tree of adder-subtractors depicted in Figure 14) and checking for arithmetic underflow. Such an encoding, however, introduces chains of exclusive-or gates. Note that exclusive-or is a non-monotonic operator (c.f. Table 1): a change of the value of a single variable occurring in a long chain of exclusive-or gates may propagate and necessitate an alteration of the values of a large number of subsequent variables in the chain (forced by unit-propagation), thus posing a challenge to contemporary satisfiability checkers.

Figure 15 shows a sorting network for two literals, an alternative way of encoding the constraint \( (\sum_i \ell_i) \leq k \) (where \( i = 2 \) in Figure 15). Intuitively, a sorting network shuffles all input values that are 1 “to the left”, i.e., if \( m \) of the inputs of an \( n \)-bit sorting
network (where \( m \leq n \)) are 1, then the output is a sequence of \( m \) ones followed by \( n - m \) trailing zeroes. To encode an “at most \( k \)” constraint it is therefore sufficient to constrain the \((k + 1)\)th output signal to 0. The advantage of this construction over the previously discussed encoding is that sorting networks can be built entirely from (mono-
tone) and-gates and or-gates (by cascading the circuit shown in Figure 15), thus avoiding
the exclusive-or gates (and the associated snowball effect caused by unit-propagation,
as described above) that retard the performance of the SAT solver. Sorting networks for
\( n \) bits can be implemented using \( O(n \cdot (\log n)^2) \) (see, for instance, [Par92]) or even
\( O(n \cdot \log n) \) gates [AKS83].

4.4. Maximum Satisfiability Problem (MAX-SAT)

Even if a formula \( F \) is unsatisfiable, there might still be assignments which satisfy a large
number of its clauses. The maximum satisfiability problem (MAX-SAT) is concerned
with finding the largest number of clauses that can be satisfied by some assignment.

**Definition 4.3 (Maximum Satisfiability Problem)** Given a formula \( F \) in conjunctive
normal form, determine the maximum number of clauses of \( F \) that can be satisfied by
some assignment.

If (and only if) the formula \( F \) is satisfiable, then there is an assignment that satisfies
all of its clauses. Accordingly, the MAX-SAT problem is NP-hard. If, however, \( F \) is
unsatisfiable, one needs to determine the largest subset of the clauses of \( F \) which, if
conjoined, are still satisfiable. Equivalently, one can compute the smallest set of clauses
that need to be dropped from the original instance to make it satisfiable.

**Example 4.1** Consider the unsatisfiable formula

\[
(\overline{r} + \overline{s} + t) \cdot (\overline{r} + s) \cdot (r) \cdot (\overline{t}) \cdot (s).
\]

(4.2)

Dropping the clause \((\overline{t})\) makes the instance satisfiable. Note that the largest set of satis-
ifiable clauses is not unique: dropping the clause \((r)\) also results in a satisfiable formula
with four clauses as well.

The partial MAX-SAT problem is a generalisation of the MAX-SAT problem, in
which some of the clauses are tagged as hard and must not be dropped.

**Definition 4.4 (Partial Maximum Satisfiability Problem)** Given a formula \( F \) and a
set \( \{C_1, \ldots, C_m\} \subseteq F \) of hard clauses, determine the maximum number of clauses of \( F \)
that can be satisfied by some assignment \( A \models C_1 \cdot C_2 \cdots C_m \).
We refer to clauses of a partial MAX-SAT instance that are not hard as soft clauses.

**Example 4.2** We revisit Example 4.1, but require that the clauses \((r)\) and \((\bar{t})\) of Formula (4.2) must not be dropped this time. In this scenario, dropping \((\bar{r} + \bar{s} + t)\) makes the formula satisfiable. Note that dropping either \((\bar{r} + s)\) or \((s)\) does not yield a satisfiable instance.

### 4.4.1. Relaxation Literals

The satisfiability checking techniques covered in Section 3 lack the ability to drop clauses. Contemporary satisfiability solvers such as MINISAT [?], however, do at least provide the option to specify a partial assignment, which can be reverted in a subsequent call to the solver without sacrificing the learnt clauses that do not depend on this assignment.

As it turns out, this mechanism is sufficient to exclude clauses from the search process if we augment these clauses with so called relaxation literals. A relaxation literal is a literal over a variable \(v\) that does not occur in the original formula. If we replace a clause \(C_i\) that is part of the original formula with the relaxed clause \((v_i + C_i)\), the literal \(v_i\) acts as a switch which enables us to activate the clause \(C_i\) by setting \(v_i\) to 0. Conversely, the solver will ignore \((v_i + C_i)\) if \(v_i\) is set to 1 (by virtue of the affirmative-negative rule introduced in Section 3.3).

**Example 4.3** We continue working in the setting of Example 4.2. The following formula resembles Formula 4.2, except for the fact that the soft clauses have been augmented with the relaxation literals \(u\), \(v\), and \(w\), respectively:

\[
(u + \bar{r} + \bar{s} + t) \cdot (v + \bar{r} + s) \cdot (r) \cdot (\bar{t}) \cdot (w + s).
\]

(4.3)

Now, any satisfiability solver can be used to determine that Formula 4.3 is satisfiable. The resulting satisfying assignment to \(u\), \(v\), and \(w\) determines which clauses were “dropped” by the solver.

Unfortunately, the technique outlined in Example 4.3 gives us no control over which, and more importantly, how many clauses the solver drops. Unless we modify the decision procedure, minimality is not guaranteed.

We can, however, restrict the number of dropped clauses by adding cardinality constraints (Section 4.3) to the relaxed formula. The corresponding constraint for the formula in Example 4.3, \((u + v + w) \leq 1\), instructs the SAT solver to drop at most one clause. Moreover, we already know that the solver has to drop at least one clause, since the original formula is unsatisfiable [MPLMS08]. In the case of Example 4.3, the SAT solver will find a satisfying solution. The rather restrictive cardinality constraint, however, does not account for (partial) MAX-SAT solutions that require the relaxation of more than one clause.

**Example 4.4** Consider the unsatisfiable formula

\[
(s) \cdot (\bar{s}) \cdot (t) \cdot (\bar{t}) .
\]
Note that this formula has two disjoint unsatisfiable cores (c.f. Section 3.8). Accordingly, the formula
\[(u + s) \cdot (v + \overline{s}) \cdot (w + t) \cdot (x + \overline{t}) \cdot (\sum \{u, v, w, x\} \leq 1)\]
is still unsatisfiable.

The formula in Example 4.4 requires the solver drop at least two clauses. This can be achieved by replacing the cardinality constraint with the slightly modified constraint \(\sum \{u, v, w, x\} \leq 2\). As outlined in Section 4.3, this can be easily achieved by modifying a single unit clause as long as we use sorting networks to encode the constraint. Moreover, such a modification does not necessarily require us to restart the search from scratch, as mentioned in the first paragraph of Section 4.4.1. Incremental satisfiability solvers (see Section 3.9) are able to retain at least some of the clauses learnt from the first instance.

Accordingly, it is possible to successively relax the cardinality constraint in an efficient manner. If we follow this scheme, we obtain an algorithm to solve the partial MAX-SAT problem. If we successively increase the numeric parameter of the cardinality constraint (by forcing one single assignment of a literal of the sorting network), starting with one, we have a solution of the partial MAX-SAT problem readily at hand as soon as the SAT solver finds a satisfying assignment.

4.4.2. Core-Guided MAX-SAT

**Example 4.5** Consider the unsatisfiable formula
\[(r + t) \cdot (r + s) \cdot (s) \cdot (\overline{s}) \cdot (t) \cdot (\overline{t})\],
which resembles the formula in Example 4.4, except for the two clauses \((r + t)\) and \((r + s)\). Neither of these clauses influences the satisfiability of the formula. Accordingly, instrumenting these clauses with relaxation literals unnecessarily introduces additional variables and increases the size of the sorting network.

It is possible to avoid this unnecessary overhead in Example 4.5 by excluding the clauses \((r + t)\) and \((r + s)\) from the set of clauses the solver considers for removal (relaxation, respectively). However, how can we know that this is sound? The exclusion of a random clause may result in an invalid answer to the MAX-SAT problem.

The answer lies in the minimal unsatisfiable cores (Definition 3.8 in Section 3.8) of the formula. A clause \(C\) that is not contained in any (minimal) unsatisfiable core of \(F\) has no impact on the satisfiability of \(F\). Accordingly, it is not necessary to instrument \(C\) with a relaxation literal. It is therefore possible to use cores to guide the selection of clauses to be relaxed [FM06] as demonstrated in the following example.

**Example 4.6** We continue working in the setting of Example 4.5. Following the method presented in Example 3.10, we obtain an initial core \{\((s), (\overline{s})\}\}. Similar to Example 4.4, we instrument the clauses occurring this core with fresh relaxation literals and impose a cardinality constraint on these literals:
\[(r + t) \cdot (r + s) \cdot (u + s) \cdot (v + \overline{s}) \cdot (t) \cdot (\overline{t}) \cdot (\sum \{u, v\} \leq 1)\]
While instance unsatisfiable, repeat:

1. Obtain unsatisfiable core \( UC \)
2. If \( UC \) contains no soft clauses, return \( UNSAT \)
3. For all soft clauses \( \{C_1, \ldots, C_n\} \subseteq UC \)
   * introduce fresh relaxation variable \( v_i \)
   * \( C_i := C_i \cup \{v_i\} \)
4. Add constraint \( \sum_{i=1}^{n} v_i \leq 1 \)
5. Obtain satisfying assignment \( A \)
6. Return number of relaxation literals \( v_i \) with \( A(v_i) = 1 \)

**Figure 16.** A core-guided MAX-SAT algorithm

This relaxation “deactivates” the core (and also overlapping non-minimal cores, which demonstrates that the core guiding our instrumentation is not required to be minimal). The modified formula (4.4), however, is still not satisfiable. It contains a second core, namely \( \{(t), (T)\} \). Defusing this core in a similar manner as the previous one yields

\[
(r+t) \cdot (r+s) \cdot (u+s) \cdot (v+\overline{v}) \cdot (w+t) \cdot (x+\overline{t}) \cdot (\sum \{u, v\} \leq 1) \cdot (\sum \{w, x\} \leq 1)
\]

A final run of the satisfiability solver yields a satisfying assignment which indicates that we need to relax two clauses. Note that it was not necessary to instrument the clauses \( (r+t) \) and \( (r+s) \) – this is a crucial advantage when it comes to large problem instances.

Figure 16 shows the pseudo-code of the core-guided MAX-SAT algorithm outlined in Example 4.6. Note that the introduction of relaxation literals complicates the use of incremental SAT algorithms (c.f. Section 3.9). At least the clauses learnt from hard constraints, however, can be retained across all instances.

### 4.5. Minimal Correction Sets (MCS)

In the previous section, the focus gradually shifted from clauses that can be satisfied simultaneously to clauses that need to be dropped to obtain a satisfiable formula. A set of clauses that has the latter property is also known as minimal correction set (MCS). The complement of each maximal set of satisfiable clauses is an MCS. Accordingly, minimal correction sets are a generalisation of the MAX-SAT problem [LS09] – as the name indicates, we merely require minimality, i.e., in general, an MCS is not minimum.

Given this close relationship between the MAX-SAT problem and MCSes, it seems natural to extend the algorithm from Figure 16 to compute correction sets. Indeed, the algorithm readily provides one MCS (whose size, in fact, is minimum). But what if we desire to compute more than one, or even all MCSes? The technique presented in [LS09] is based on the algorithm in Section 4.4.2 and relies on blocking clauses (see Section 4.1) to exhaustively enumerate all minimal correction sets.

The algorithm in Figure 17 uses several auxiliary helper functions which implement techniques we have encountered in the previous sections.

- The procedure \textsc{Instrument} adds relaxation literals to clauses of the formula provided as parameter. If no second parameter is provided, the procedure instru-
Algorithm 1. A core-guided algorithm to compute MCSes

1. $k := 1$
2. MCSes := ∅
3. UC$_k$ := unsatisfiable core of $F$
4. While (INSTRUMENT($F$) · (BLOCK(MCSes))) is satisfiable
   1. Instrument clauses in UC$_k$ with relaxation literal:
      $F_k :=$ INSTRUMENT($F$, UC$_k$) · ATMOST($k$, UC$_k$)
   2. Enumerate satisfying assignments to relaxation variables:
      MCSes := MCSes ∪ ALLSAT($F_k$ · BLOCK(MCSes))
   3. UC$_{k+1}$ := UC$_k$ ∪ core of $F_k$ · BLOCK(MCSes)
      (projected to clauses of $F$)
   4. $k := k + 1$
5. return MCSes

Figure 17. A core-guided algorithm to compute MCSes

...
algorithm presented in Section 3.8, the satisfiability solver returns the unsatisfiable core \( \{ (\tau + \bar{\tau} + t), (r), (\bar{\tau}), (s) \} \). Accordingly, the algorithm constructs the formula
\[
(u + \tau + \bar{\tau} + t) \cdot (\tau + s) \cdot (v + r) \cdot (w + \bar{\tau}) \cdot (x + s) \cdot (\sum \{ u, v, w, x \} \leq 1)
\]

Then, it incrementally constructs all satisfying assignments to \( \{ u, v, w, x \} \) that are consistent with this formula. We obtain the partial assignments
\[
\{ u \mapsto 1, v \mapsto 0, w \mapsto 0, x \mapsto 0 \}, \quad \{ u \mapsto 0, v \mapsto 1, w \mapsto 0, x \mapsto 0 \}, \text{ and } \{ u \mapsto 0, v \mapsto 0, w \mapsto 1, x \mapsto 0 \}.
\]

and the corresponding blocking clauses \((\bar{\pi}), (\bar{\pi}), \text{ and } (\bar{w})\). The respective MCSes of cardinality one are \( \{ (\tau + \bar{\tau} + t) \}, \{ r \}, \text{ and } \{ \bar{\tau} \} \). Note that the partial assignment \( \{ u \mapsto 0, v \mapsto 0, w \mapsto 0, x \mapsto 1 \} \) is not a satisfying assignment, since dropping the clause \( (s) \) does not make the formula satisfiable – the unit clause \( (s) \) can be inferred from \( (\tau + s) \) and \( (r) \). After blocking all MCSes (controlled by the variables \{ u, v, w, x \}), we end up with the formula
\[
(u + \tau + \bar{\tau} + t) \cdot (\tau + s) \cdot (v + r) \cdot (w + \bar{\tau}) \cdot (x + s) \\
\cdot (\sum \{ u, v, w, x \} \leq 1) \cdot (\bar{\pi}) \cdot (\bar{\tau}) \cdot (\bar{w}).
\]

In step 3, the algorithm constructs the core of this formula, replaces the instrumented clauses with their original counterparts, and drops the cardinality constraint and the blocking clauses from the core. We obtain the new core
\[
\{ (\tau + \bar{\tau} + t), (\tau + s), (r), (\bar{\tau}) \}.
\]

Note that, since the blocking clauses do not prevent \( (s) \) from being dropped, the clause \( (\tau + s) \) must be contained in this core.

In the next step, the algorithm increases \( k \). Now, all clauses have to be instrumented (since the union of both cores computed so far happens to be the set of all clauses of the original formula), and all MCSes computed so far need to be blocked. In combination with the new cardinality constraint, we obtain
\[
(u + \tau + \bar{\tau} + t) \cdot (y + \tau + s) \cdot (v + r) \cdot (w + \bar{\tau}) \cdot (x + s) \cdot (\bar{\pi}) \cdot (\bar{r}) \cdot (\bar{w}) \\
(\sum \{ u, v, w, x, y \} \leq 2).
\]

Since neither dropping \( (s) \) nor dropping \( (\tau + s) \) from the original instance makes the formula satisfiable, the algorithm determines the satisfying assignment \{ u \mapsto 0, y \mapsto 1, v \mapsto 0, w \mapsto 0, x \mapsto 1 \}. This assignment is in fact the only satisfying partial assignment to the variables \{ u, v, w, x, y \} for the given formula. The corresponding blocking clause is \( (\tau + \bar{\tau}) \).

We leave it to the reader to verify that \textsc{Instrument}(F) \cdot (\bar{\pi}) \cdot (\bar{\tau}) \cdot (\bar{w}) \cdot (\tau + \bar{\tau}) \) in line 3 is now unsatisfiable, and that the algorithm therefore terminates reporting the MCSes.
4.6. Minimal Unsatisfiable Cores

We observed in Section 4.5 that a minimal correction set comprises clauses that need to be dropped to “defuse” all unsatisfiable cores of a formula. Conversely, choosing at least one clause from each minimal correction set of a formula yields an unsatisfiable core. The following definition enables us to formalise this observation.

Definition 4.5 (Hitting Set) Given a set of sets \( S \), a hitting set of \( S \) is a set \( H \) such that

\[
\forall S \in S. H \cap S \neq \emptyset
\]

Minimal correction sets and unsatisfiable cores are dual [LS08] in the following sense:

- Let \( S \) be the set of all MCSes of an unsatisfiable formula \( F \). Then each (minimal) hitting set of \( S \) is a (minimal) unsatisfiable core (see Section 3.8).
- Let \( S \) be the set of all minimal unsatisfiable cores of an unsatisfiable formula \( F \). Then each (minimal) hitting set of \( S \) is a (minimal) correction set for \( F \).

The following example illustrates this duality.

Example 4.8 The leftmost column in Figure 18 shows the set of all minimal correction sets \( \{((\overline{s})), \{(r), (s)\}, \{(s), (\overline{r}+s)\}\} \) for the unsatisfiable formula

\[
F \equiv (\overline{s}) \cdot (\overline{r}+s) \cdot (r) \cdot (s).
\]

The check-marks in the table indicate the occurrences of the clauses of \( F \) in the respective MCS. By choosing a subset of clauses of \( F \) which “hit” all MCSes, we obtain a minimal unsatisfiable core. The formula \( F \) has two minimal unsatisfiable cores, namely \( \{(s), (\overline{s})\} \) and \( \{(r), (\overline{s}), (\overline{r}+s)\} \). The choice of appropriate “hitting” clauses is indicated in Figure 18 by oval and rectangular boxes, respectively.

The problem of deciding whether a given set of sets has a hitting set of size \( k \) (or smaller) is NP-complete ([Kar72] in [LS08]). An algorithm optimised for the purpose of extracting cores from sets of MCSes can be found in [LS08].
Instead of presenting the algorithm suggested in [LS08], we draw the readers attention to the fact that after the final iteration of the algorithm in Figure 17, the set of clauses (\textsc{block}(MCSes)) in step $\$ is a \textit{symbolic} representation of all minimal correction sets. Essentially, we are looking for assignments that satisfy the CNF formula (\textsc{block}(MCSes)). Note that the phase of all literals in (\textsc{block}(MCSes)) is negative, since the respective clauses block assignments of 1 to relaxation variables. Accordingly, in order to find minimal unsatisfiable cores, we need to minimise the number of variables set to 0 in the satisfying assignment to (\textsc{block}(MCSes)). Again, this can be achieved by means of gradually relaxed cardinality constraints.

\textbf{Example 4.9} In Example 4.7, we ended up with the blocking clause
\[(\overline{u}) \cdot (\overline{v}) \cdot (\overline{w}) \cdot (x + y),\]
where the relaxation literals $u$, $v$, $w$, $x$, and $y$ correspond to the clauses $(\overline{r} + \overline{s} + t)$, $(r)$, $(\overline{t})$, $(s)$, and $(r + s)$, respectively. Each of the clauses is satisfied if at least one of its literals evaluates to 1 (and the corresponding variable evaluates to 0, respectively). In order to find a minimal hitting set, we constrain the literals using a cardinality constraint:
\[(\overline{u}) \cdot (\overline{v}) \cdot (\overline{w}) \cdot (x + y) \cdot \left(\sum \{u, v, w, x, y\} \leq k\right)\]

Note that $k$ has to be at least four, since there are four clauses which do not share any literals. This threshold can be obtained using a syntactical analysis of the formula or simply by incrementally increasing $k$ until it is sufficiently large.

If we generate all minimal satisfying assignments to the constrained formula (using blocking clauses in a way similar to Example 4.7) we obtain the following assignments for $k = 4$:
\begin{itemize}
  \item $\{\overline{u} \mapsto 1, \overline{v} \mapsto 1, \overline{w} \mapsto 1, \overline{x} \mapsto 1, y \mapsto 0\}$ and
  \item $\{\overline{u} \mapsto 1, \overline{v} \mapsto 1, \overline{w} \mapsto 1, \overline{x} \mapsto 0, y \mapsto 1\}$
\end{itemize}

These assignments correspond to the minimal unsatisfiable cores
\begin{itemize}
  \item $\{(\overline{r} + \overline{s} + t), (r), (\overline{t}), (s)\}$
  \item $\{(\overline{r} + \overline{s} + t), (r), (\overline{t}), (r + s)\}$
\end{itemize}

The hitting set problem is equivalent to the set cover problem, an NP-complete problem that has been extensively studied in complexity theory. We do not claim that the technique in Example 4.9 is competitive compared to other algorithms such as the one presented in [LS08] – the purpose of the example is to gain a deeper understanding of hitting sets.

The following section discusses examples of applications of the techniques presented in Sections 3 and 4.
5. Applications in Automated Verification

Contemporary SAT solvers are the enabling technology for a number of successful verification techniques. Bounded Model Checking, for instance, owes its existence to a large extent to the impressive advances of satisfiability solvers. This section presents – without claiming completeness in any way – a number of examples of how SAT solvers are applied in contemporary verification tools. After discussing how propositional logic can be used to represent circuits and software programs (Section 5.1), we discuss automated test-case generation (Section 5.2), Bounded Model Checking (Section 5.3), and fault localisation (Section 5.4).

5.1. Encoding Circuits and Programs

There is a natural correspondence between combinational circuits, such as the full-adder in Figure 14(b), and propositional logic formulae. Accordingly, the encoding of the circuit in Figure 14(b) is straightforward:

\[
(a_1 \leftrightarrow (a \cdot b)) \cdot (o_2 \leftrightarrow (a \oplus b)) \cdot (o_3 \leftrightarrow (o_2 \cdot c_i)) \cdot (s \leftrightarrow (o_2 \oplus c_i)) \cdot (c_o \leftrightarrow (o_1 + o_3))
\]

(5.1)

As described in the first step of Tseitin’s encoding (presented in Section 2.1.2), the encoding introduces fresh variables \(o_1, o_2, o_3\) that represent the inner signals and wires of the circuit that do not correspond to inputs or outputs. Based on Formula 5.1, we can construct a relation \(R\) which maps valuations to the input signals to the corresponding output signals:

\[
R(a, b, s, c_i, o_1, o_2, o_3) \overset{\text{def}}{=} \exists o_1 o_2 o_3 \cdot \left((o_1 \leftrightarrow (a \cdot b)) \cdot (o_2 \leftrightarrow (a \oplus b)) \cdot (o_3 \leftrightarrow (o_2 \cdot c_i)) \cdot (s \leftrightarrow (o_2 \oplus c_i)) \cdot (c_o \leftrightarrow (o_1 + o_3))\right)
\]

(5.2)

Any satisfying assignment to this relation \(R\) (or to Formula 5.1, respectively) represents a possible combination of input/output signals, e.g.,

\[
a \mapsto 0, \ b \mapsto 1, \ c_i \mapsto 1, \ s \mapsto 0, \ c_o \mapsto 1
\]

corresponds to the case in which the full-adder yields a sum of zero and a set carry-out bit for an input of 0 and 1 and a carry-in bit of value 1. The transition relation \(R\) (5.2) is a symbolic encoding of all possible input/output pairs of the full-adder.

In a sequential circuit (see Figure 19(a)), the relation \(R\) encodes one execution cycle of the circuit. It is possible to extend this representation to a fixed number of \(k\) execution cycles by replicating (or unfolding) the combinational part of the circuit \(k\) times. The unfolding yields an iterative logic array [ABF90] (as illustrated in Figure 19(b) for two cycles). For each time-frame \(t\), we introduce a fresh set of variables (as indicated by the super-script \(t\)). The initial state of the circuit imposes no constraints on the internal signals: their value can be either 1 or 0 (indicated by \(*\) in Figure 19(b)).

Figure 19 shows a simple example of such an unfolding. The sequential circuit in Figure 20(a) has two input signals \(i_1\) and \(i_2\) and one output signal \(o\). In the corresponding
2-cycle unfolding in Figure 20(b) we introduce a fresh variable for each of these signals in each execution cycle (e.g., $i_1^1$, $i_2^1$, ...).

By means of Tseitin’s transformation (Section 2.1.2) we obtain the propositional representation in Figure 21 of the unfolded circuit in Figure 20(b) in conjunctive normal form. The clauses in Figure 21 are grouped with respect to the gates and cycles by which they are contributed.

Each satisfying assignment of this formula represents a feasible execution of two cycles of the sequential circuit in Figure 20(a). In general, $k$ cycles are encoded by $k$ instances of the relation $R$:

$$R(i_1^1, o_1^1) \cdot R(i_2^1, o_2^1) \cdot \cdots \cdot R(i_k^1, o_k^1)$$

(5.3)

(where $i_t^t, o_t^t$ represents the input and output variables of time-frame $t$).

Software programs can be encoded in a similar manner. The semantics of each instruction of a program is determined by the hardware implementation of the operators
that occur in the instruction. The addition of two 4-bit variables $a$ and $b$, for instance, can be encoded using the ripple-carry adder in Figure 14(a). Accordingly, each $n$-bit variable $a$ in the program is encoded using $n$ propositional variables representing the $n$ bits of $a$; this technique is known as bit-flattening or bit-blasting. We refer the reader to [KS08] for a detailed treatment of various operators of common imperative programming languages such as ANSI-C or Java.

Accordingly, an instruction at the program location $\ell$ of the given program can be represented using a propositional relation $R_\ell(\vec{v}_i, \vec{v}_j)$, where $\vec{v}_i$ refers to the propositional variables representing the program state before the execution of the instruction and $\vec{v}_j$ refers to the variables representing the state after the execution. To avoid notational clutter, we refrain from using the bit-level representation of program instructions and will deploy a more abstract notation for transition relations (such as $R_\ell(x^i, x^j) \overset{\text{def}}{=} (x^j = x^i + 1)$ for the instruction $x++$ at location $\ell$).

Unlike circuits, which are executed in a synchronous manner, software programs typically have a control flow structure which determines which instruction is executed at which point in time. Figure 22(a), for instance, illustrates the control flow graph (CFG) of the conditional instruction $\text{if } (x \% 2) \{ x = x \times 2; \} \text{ else } \{ x = x - 1; \}$. Accordingly, it is not sufficient to simply encode all instructions as propositional relations; one also has to take the control flow of the program into account.

In Figure 22(a), the variable $x$ is assigned in two different branches of the conditional statement. We cannot simply use the same propositional variables to represent the value of $x$ in each branch, since this would result in an unsatisfiable formula ($x$ cannot take two values at the same time). Therefore, we need to guarantee, that different versions of the variables are used in each branch. This can be achieved by transforming the program into the static single assignment (SSA) form [CFR+91]. The SSA form of a program is an intermediate representation used in compiler construction which guarantees that each variable is assigned exactly once. This property is achieved by replacing existing variables in the original program with fresh variables such that the right-hand side of each assignment in the program gets its own version of the assigned variable. The SSA form of the program fragment in Figure 22(a) is shown in Figure 22(b). In the SSA form, the assignment $x^3 = \phi(x^1, x^2)$ indicates a join of two branches of the program. At this point the variable $x^3$ needs to be assigned the value of either $x^1$ or $x^2$, depending on which branch was executed. It is, however, impossible to determine statically which branch modifies $x$. Therefore, we encode the control flow dependency into the transition relation as follows:

![Figure 22. Encoding the control flow of software programs](image-url)
(a) A CFG with a loop
(b) An unrolled CFG

Figure 23. Unwinding loops in software programs

\[
\text{while } (x) \quad \rightarrow \quad \text{if } (x) \{ \\
\quad \text{BODY;} \\
\quad \text{if } (x) \\
\quad \text{BODY;} \\
\quad \text{else} \\
\quad \text{exit ();} \\
\}
\]

In this formula, the value of \(x^3\) depends on the value of \(x^0\), the version of the variable \(x\) representing the value of \(x\) before the execution of the conditional statement.

Repetitive constructs (such as loops) can be treated similar to the encoding of execution cycles of a hardware circuit. However, instead of unwinding the entire transition relation of the program, each loop is unwound separately up to a pre-determined bound. Syntactically, this corresponds to a replication the loop body and the appropriate guard (Figure 24). The unwinding is illustrated in Figure 23. The CFG on the left side (Figure 23(a)) represents a simple program with a single loop. The graph on the right side (Figure 23(b)) illustrates the structure resulting from unwinding the loop body between the program locations \(L_3\) and \(L_4\) twice. The size of the resulting unwound program is linear in the size of the original program and the depth of the unwinding. Alternative unwinding techniques are discussed in the survey [DKW08]. After transforming the resulting unwound program into SSA, the bounded instance can be encoded as a propositional formula as before. The resulting formula effectively simulates all possible executions up to the pre-determined unwinding depth of the loops in the program. Accordingly, this technique is also known as symbolic simulation [Kin70].
5.2. Test-Case Generation

The fact that a bounded unwinding of a circuit design or a program symbolically encodes all possible executions up to a certain depth $k$ makes it an ideal tool for automated test-case generation: each satisfying assignment generated by a SAT solver corresponds to a test scenario. In this setting, the circuit design or program takes the role of a specification; the resulting test-cases are used to verify the actual integrated circuit or a compiled version of the program. There is one subtle pitfall: a test-case extracted from the source code of the actual program (or chip design) under test must necessarily succeed if the compiler (or synthesis tool) is correct. It is therefore common practice to extract test-cases from a model or abstract specification of the artifact under test. With the rise of model-based development (MBD) methodologies such models are available increasingly often. In [BHM+ 10], for instance, test-cases are extracted from Simulink models. In combination with an incremental SAT solver it is possible to generate an entire suite of test-cases which satisfies certain coverage criteria such as path coverage or modified condition/decision coverage (MC/DC): the coverage criteria are simply encoded as constraints, and previously generated test-cases are barred by means of blocking clauses [HSTV08,HSTV09].

The test-case generator described in [BHM+ 10], for instance, deploys mutations as a coverage criterion. A mutation is a small modification – such as using a wrong operator or variable name – to the original design or source code. A test suite which does not detect the injected fault is considered insufficient. Instead of using mutations to evaluate a given test-suite, however, [BHM+ 10] uses mutations as a catalyst to generate a test-suite which, by construction, covers all injected faults. To this end, the test-generation algorithm contrasts the unwound transition relation of the mutated (original) source code with the original unwound transition relation. Let $R^k_m$ ($R^k$, respectively) denote the relation encoding $k$ unwindings of the mutated (original) transition relation, respectively. The test-case generator then constructs the following formula:

$$R^k(i^1, o^k) \cdot R^k_m(i^1, m^k) \cdot ((o^k_1 \oplus m^k_1) + (o^k_2 \oplus m^k_2) + \cdots + (o^k_n \oplus m^k_n)) . \quad (5.4)$$

Observe that the input variables for both the original as well as the mutated transition relations are the same. A so called miter enforces that Formula 5.4 is only satisfiable if the valuation to the input variables yields output values $o^k$ and $m^k$ for the two different transition relations which disagree on at least one value. This approach (which is based on equivalence checking) guarantees that the resulting test case detects the faults injected in $R^k_m$.

**Example 5.1** Consider the mutated version (depicted in Figure 25) of the circuit in Figure 20(b). Note that the “and”-gate in the first cycle has been replaced with an “or”-gate, and that all output and internal signals were renamed. The input signals $i_1^1$, $i_2^1$, $i_1^2$, $i_2^2$, and the signal $s$ representing the initial state of the latch remain unchanged.

We obtain the following encoding in conjunctive normal form:

- **cycle 1**
  - $(r^1 i_1^1) \cdot (r^1 \pi) \cdot (i_1^1 s \pi r^1) \cdot (i_2^1 m^1) \cdot (\pi m^1) \cdot (m^1 i_2^1 s)$
- **cycle 2**
  - $(\pi i_1^2) \cdot (\pi r^1) \cdot (i_1^2 r^1 t) \cdot (i_2^2 m^2) \cdot (\pi m^2) \cdot (m^2 i_2^2 r^1)$
Figure 25. A mutated version of the circuit in Figure 20(b).

The miter \((o^1 \oplus m^1) + (o^2 \oplus m^2)\) enforces that any assignment satisfying the conjunction of the formula representing the original circuit and the formula representing the mutated circuit yields different values for at least one output. The reader may verify that \(o^2\) and \(m^2\) must take different values in any extension of the partial assignment

\[
\begin{align*}
& s \mapsto 0 & i_1 \mapsto 1 & i_2 \mapsto 0 & i_1 \mapsto 0 & i_2 \mapsto 0
\end{align*}
\]

to a total assignment. Accordingly, the corresponding test-case detects the incorrect “or”-gate.

5.3. Bounded Model Checking

Model checking [CGP99] is a technique that explores all reachable states of a model to check whether a given property is satisfied. Unlike testing, model checking performs an exhaustive search of the state space and provides a correctness guarantee that is rarely achieved by means of testing. Moreover, if the specification is violated, model checking tools are able to provide a counterexample, i.e., a witness demonstrating how the property in question can be violated.

Bounded model checking (BMC) [BCCZ99] is a variation of model checking which restricts the exploration to execution traces up to a certain (user-defined) length \(k\). BMC either provides a guarantee that the first \(k\) execution steps of the model satisfy the property \(P\) or a counterexample of length at most \(k\). This setting should sound familiar to the reader: Section 5.1 describes how all execution traces up to depth \(k\) can be encoded in a propositional formula. Given such an encoding, it is sufficient to augment each execution cycle with a formula encoding the negation of the property \(P\). This is indicated in the following diagram (here, \(I\) denotes a constraint encoding the valid initial states of the model):

\[
\begin{align*}
& I \quad R & I \quad R & \cdots & I \quad R
\end{align*}
\]

Any assignment satisfying the resulting formula represents a counterexample to the claim that \(P\) holds. If the formula is unsatisfiable, on the other hand, then the claim holds in the first \(k\) execution steps. An example for a bounded model checking tool for programs written in the ANSI-C language is CBMC [CKL04].

5.4. Fault Localisation

The techniques discussed in Section 5.2 and Section 5.3 are aimed at discovering bugs in software and hardware designs. Finding a bug, however, is just the first step. Localising and understanding the underlying fault is often a much more daunting task.
Accordingly, automated support for fault localisation is highly desirable. In this section, we discuss how MAX-SAT and minimal correction sets can be applied to localise bugs. This approach, also known as consistency-based diagnosis, has been successfully applied to localise faults in hardware designs (see, for instance, [SMV+07, SFBD08, CSVMS09, CSMSV10, ZWM11]) as well as in software [JM11].

Consistency-based diagnoses aims at identifying the fractions of the hardware design or the source code of the software that are inconsistent with an observed (or expected) behaviour. We distinguish two scenarios:

1. The transition relation $R$ (obtained from the source code or hardware design) represents the implementation of the artifact under test and an observed behaviour of this implementation contradicts the specification (e.g., the requirements document or a use case scenario). This setting is addressed in [SMV+07, SFBD08, CSVMS09, CSMSV10, JM11], for instance.

2. The transition relation $R$ represents the specification of the artifact under test. The observed behaviour (e.g., a test run of a manufactured integrated circuit) is inconsistent with $R$. This scenario is addressed in [ZWM11].

In the first case we assume that the specification is given as a set of constraints or an assignment to the input and output variables of the transition relation $R$. In the second case we assume that the observed test scenario is provided as an assignment to the variables of $R$. While the two scenarios are in a sense dual, the objective in both cases is to identify the “elements” of the transition relation $R$ that are inconsistent with the observed (or expected) behaviour. In both cases, we have to specify what we mean by “elements” – this is determined by the underlying fault model. The notion of a fault model is similar to the concept of a mutation, discussed in Section 5.2. A fault model determines which and how components of the transition relation can possibly fail. A gate in an integrated circuit, for instance, may malfunction and constantly yield an output value of 1 – this fault is known as stuck-at-constant. In a program, the developer may accidentally use the instruction $y=x++$ instead of $y=++x$, which results in an incorrect value of the variable $y$. The faulty element is the respective gate in the first case and the respective line of code in the second case. In both cases, we would like to automatically pinpoint the location of the fault.

In the following, we consider only a rather simplistic fault model for hardware as well as for software: we assume that the output of a gate or the result of an assignment may be an arbitrary value. The motivation is that this fault model can be easily encoded in the transition relation $R$ by means of relaxation literals (c.f. Section 4.4.1). By relaxing the set of clauses that encode the output value $o_i$ of a gate or an assignment of an SSA variable $x_i$ we effectively cut the signal or variable loose. The following two examples illustrate how minimal correction sets enable us to locate faults in this setting.

**Example 5.2** We work in scenario 1 described above. The code fragment in SSA in Figure 26 represents the implementation of a program. We assume that the specification of the software states that the value of $y$ must be even after the execution of the conditional statement. This requirement is represented by the constraint $(y^0 \mod 2 = 0)$ and obviously violated if $x^0$ is odd. Assume that the test engineer reports that the requirement does not hold for $x^0 = 1$. By combining the constraint and the assignment with the encoding of the program we obtain the formula
Figure 26. A conditional statement with a faulty branch

\[
\begin{align*}
[x^0%2 = 0] & \quad [x^0%2 = 1] \\
y^1 = x^0 & \cdot 2 \\
y^2 = x^0 & \\
y^3 = \phi(y^1, y^2) & \\
x^1 = x^0 & + 1 \\
x^2 = \phi(x^0, x^1)
\end{align*}
\]

Notably, this formula is unsatisfiable; for the given input the transition relation does not satisfy the requirement. In order to fix the bug, the developer needs to locate the fault. In accordance with the simplistic fault model suggested above, we assume that one of the assignments \(y^1 = x^0 \cdot 2\) or \(y^2 = x^0\) (represented by the expressions \((x^0%2 = 0) \cdot (x^2 = x^0) \cdot (y^1 = y^1)\) + \((x^0%2 = 1) \cdot (x^2 = x^1) \cdot (y^3 = y^2)\)) are at fault. In order to locate the fault, we mark the propositional clauses encoding these expressions as soft clauses and compute all minimal correction sets for the resulting formula. Note that, in accordance with our fault model, the conditions \((x^0%2 = 0)\) and \((x^0%2 = 1)\) are represented by hard clauses and may not be dropped. Moreover, the constraints \((x^0 = 1) \cdot (y^3%2 = 0)\) representing the test scenario and the requirement must not be relaxed, either, since changing the test scenario or the requirements is an undesired solution to the problem.

Using the algorithm described in Section 4.5, we can now compute the minimal correction sets for the problem instance described above. The \((y^2 = x^0)\) is identified as the culprit and helps the developer to narrow down the fault location to the instruction \(y = x++\).

**Example 5.3** In Scenario 2, the behaviour of the test artifact does not comply with the specification represented by \(R\). This situation may arise in the context of post-silicon validation, for instance: the manufacturing process may introduce a fault in the prototype of a chip, resulting in a discrepancy of the behaviour of the integrated circuit and its design. Debugging an integrated circuit is non-trivial, since unlike in software debugging, its internal signals can not be easily observed.

Consider the sequential circuit in Figure 20(a). After resetting the latch, we expect the output \(o\) to remain 0 as long as the input signal \(i_2\) is constantly 0. Assume, however, that we observe an output value of 1 after two cycles when executing the described scenario on the chip. Figure 20(b) depicts a two-cycle unfolding of the circuit. Figure 21 shows the corresponding CNF encoding. Assume that we observe and record the values \(o^1 \rightarrow 0\) and \(o^2 \rightarrow 1\) during a test-run with the initial state \(s \rightarrow 0\) and the stimuli \(i^1_2 \rightarrow 0\), and \(i^2_2 \rightarrow 0\). Note that we have no information about the signal \(i^1\). These observations contribute the hard constraint \(o^1 \cdot o^2 \cdot i^1_2 \cdot i^2_2\), which is not satisfiable in conjunction with the formula in 21. Using a \textsc{Max-SAT} solver, we can derive that the conjunction becomes
satisfiable if we drop either \((\overline{t_1})\) or \((\overline{o_2} s_2 t_1)\) (both of which are an MCS) from 21. Accordingly, either the “and”-gate in cycle one or the “or”-gate in cycle two must have defaulted. Notably, our fault localisation technique managed to narrow down the set of possibly faulty gates without knowledge about the internal signals of the physical circuit. Fault localisation in silicon debug is addressed in more detail in [ZWM11].

6. Conclusion

The advances of contemporary SAT solvers have transformed the way we think about NP complete problems. They have shown that, while these problems are still unmanageable in the worst case, many instances can be successfully tackled. In Section 3, we discussed the main contributions and techniques that made this paradigm shift possible. Section 4 covers a number of natural extensions to the SAT problem, such as the enumeration all satisfying assignments (ALL-SAT) and determining the maximum number of clauses that can be satisfied by an assignment (MAX-SAT). SAT solvers and their extensions have immediate applications in domains such as automated verification, as discussed in Section 5. In fact, many successful verification techniques such as Bounded Model Checking owe their existence to the impressive advances of modern SAT solvers. While SAT solvers can easily be used as a black box, the realisation of many of these applications relies on internal features of SAT solvers and requires an in-dept understanding of the underlying algorithms.

SAT solvers are still improving at an impressive rate (as demonstrated by the results of the annual SAT solver competition – http://www.satcompetition.org/) and novel applications are conceived and published on a regular basis.

7. Acknowledgements

The authors are indebted to Matthias Schlaipfer and the attendees of the Summer School Marktberdoll 2011 for their comments on this tutorial.
A. Exercises

Exercise 1 Use Tseitin’s transformation to convert $x + (y \cdot (\overline{z} \oplus x))$ into CNF.

Solution By introducing the following fresh variables

$$w, q, u, v$$

we obtain the formula

$$w \cdot (q \leftrightarrow (z \cdot x)) \cdot (p \leftrightarrow (\overline{z} \cdot \overline{x})) \cdot (u \leftrightarrow (p + q)) \cdot (v \leftrightarrow (y \cdot u)) \cdot (w \leftrightarrow (x + v))$$

We can now apply the rules

(A.1) $a \leftrightarrow (b + c) \equiv (\overline{b} + a) \cdot (\overline{c} + a) \cdot (\overline{a} + b + c)$

(A.2) $a \leftrightarrow (b \cdot c) \equiv (\overline{a} + b) \cdot (\overline{a} + c) \cdot (\overline{b} + \overline{a} + a)$

and get

$$w \cdot (\overline{q} + z) \cdot (\overline{q} + x) \cdot (\overline{z} + \overline{x} + q) \cdot (\overline{p} + \overline{x}) \cdot (\overline{p} + \overline{x}) \cdot (z + x + p) \cdot$$

$$\quad (\overline{p} + u) \cdot (\overline{q} + u) \cdot (\overline{u} + p + q) \cdot (\overline{v} + v) \cdot (\overline{v} + y + u) \cdot$$

$$\quad (\overline{v} + w) \cdot (\overline{v} + w) \cdot (\overline{w} + x + v)$$

Exercise 2 Follow the scheme in Table 2 in Section 2.1.2 to derive the Tseitin clauses that characterise the n-ary Boolean formulas $(y_1 + y_2 + \cdots + y_n)$ and $(y_1 \cdot y_2 \cdots \cdot y_n)$.

Solution

- Disjunction:

  $$x \leftrightarrow (y_1 + y_2 + \cdots + y_n)$$
  $$\equiv (x \rightarrow (y_1 + y_2 + \cdots + y_n)) \cdot ((y_1 + y_2 + \cdots + y_n) \rightarrow x)$$
  $$\equiv (\overline{x} + y_1 + y_2 + \cdots + y_n) \cdot ((y_1 \rightarrow x) \cdot (y_2 \rightarrow x) \cdots (y_n \rightarrow x))$$
  $$\equiv (\overline{x} + y_1 + y_2 + \cdots + y_n) \cdot (\overline{y}_1 + x) \cdot (\overline{y}_2 + x) \cdots (\overline{y}_n + x)$$

- Conjunction:

  $$x \leftrightarrow (y_1 \cdot y_2 \cdots \cdot y_n)$$
  $$\equiv (x \rightarrow (y_1 \cdot y_2 \cdots \cdot y_n)) \cdot ((y_1 \cdot y_2 \cdots \cdot y_n) \rightarrow x)$$
  $$\equiv ((\overline{x} + y_1) \cdot (\overline{x} + y_2) \cdots \cdot (\overline{x} + y_n)) \cdot ((y_1 \cdot y_2 \cdots \cdot y_n) + x)$$
  $$\equiv ((\overline{x} + y_1) \cdot (\overline{x} + y_2) \cdots \cdot (\overline{x} + y_n)) \cdot (\overline{y}_1 + \overline{y}_2 + \cdots + \overline{y}_n + x)$$
Exercise 3 Which of the Boolean formulae below are satisfiable, and which ones are unsatisfiable?

1. \( x + x \cdot y \)
2. \( (x \cdot (x \rightarrow y)) \rightarrow y \)
3. \( x \cdot ((x \rightarrow y) \rightarrow y) \)

Convert the formulae that are unsatisfiable into conjunctive normal form (either using Tseitin’s transformation or the propositional calculus) and construct a resolution refutation proof.

Solution

• satisfiable: 1, 3
• unsatisfiable: 2

\[
(x \cdot (x \rightarrow y)) \rightarrow y \equiv (x \cdot (\overline{x} + y)) + y \\
\equiv (x) \cdot (\overline{x} + y) \cdot (\overline{y})
\]

Resolution proof:

\[
\text{Res}((\overline{y}), \text{Res}((x), (\overline{x} + y), x), y) \equiv \square
\]

Exercise 4 Construct a resolution refutation graph for the following unsatisfiable formula:

\[
y_1 \cdot y_2 \cdot y_3 \cdot (y_1 + x) \cdot (y_2 + \overline{x} + z) \cdot (y_3 + \overline{z}) \cdot y_4
\]

Solution The resolution graph for Exercise 4 is shown in Figure 27.

![Resolution Graph for Exercise 4](image)

Exercise 5 Apply the rules of the Davis-Putnam procedure (outlined in Section 3.3) to the following formula until you obtain an equi-satisfiable formula that cannot be reduced any further:

\[
y_1 \cdot y_2 \cdot (\overline{y}_1 + x + \overline{z}) \cdot (\overline{y}_2 + \overline{x} + z) \cdot (y_3 + \overline{z}) \cdot y_4
\]
Solution  We perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Rule</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1-literal-rule on $y_1$</td>
<td>$y_2 \cdot (x + \overline{z}) \cdot (\overline{y}_2 + \overline{x} + z) \cdot (y_3 + \overline{z}) \cdot y_4$</td>
</tr>
<tr>
<td>2</td>
<td>1-literal-rule on $y_2$</td>
<td>$(x + \overline{z}) \cdot (\overline{y} + z) \cdot (y_3 + \overline{z}) \cdot y_4$</td>
</tr>
<tr>
<td>3</td>
<td>Affirmative-negative</td>
<td>$(x + \overline{z}) \cdot (\overline{y} + z)$</td>
</tr>
<tr>
<td>4</td>
<td>Resolution on $x$</td>
<td>$(z + \overline{z})$</td>
</tr>
</tbody>
</table>

The resulting formula $(z + \overline{z})$ is a tautology and cannot be eliminated by any of the Davis-Putnam rules. Accordingly, the original formula must be satisfiable.

**Exercise 6** Apply the Davis-Putnam-Logeman-Loveland (DPLL) procedure (described in Section 3.4) to the following formula:

$$y_1 \cdot y_2 \cdot (\overline{y}_1 + x + z) \cdot (\overline{y}_2 + x + z) \cdot (y_3 + \overline{z}) \cdot (y_4 + \overline{z})$$

Solution  Table 6 shows one possible scenario. Note that there is no value of $x$ that satisfies the formula. The reader may verify that choosing a decision variable other than $x$ in the third step also yields a contradiction.

**Exercise 7** Simulate the conflict-driven clause learning algorithm presented in Section 3.5 on the following formula:

$$C_0 = (x + y + z) \cdot (x + z) \cdot (x + y + \overline{z}) \cdot (x + \overline{y} + z) \cdot (x + y + \overline{z}) \cdot (x + y + z)$$
Solution It is obvious that one has to make at least two decisions before one of the clauses becomes unit. If we start with the decisions $x \oplus 1$ and $y \oplus 2$, we obtain the implication graph in Figure 28.

By means of resolution (c.f. Section 3.6) we obtain the conflict clause $C_8 \equiv \text{Res}(C_0, C_1, z) \equiv (\overline{x} + \overline{y})$. We revert all decisions up to (but excluding) level 1, which is the second-highest decision level occurring in $C_8$. The clause $C_8$ is unit under the assignment $x \oplus 1$, thus implying the assignment $y \oplus 1$. We obtain the implication graph in Figure 29. Again, there is a conflict.

The resulting conflict clause is $C_9 \equiv \text{Res}(C_8, \text{Res}(C_2, C_3, z), y) \equiv (\overline{x})$, forcing us to revert to decision level zero and set $x$ to 0. Under this assignment, none of the clauses is unit and we have to make a choice for either $y$ or $z$. If we choose $y \oplus 1$, the clause $C_4$ becomes assertive and forces us to assign 0 to $z$. This assignment, however, is in conflict with $C_5$, and by means of resolution we obtain the conflict clause $C_{10} \equiv \text{Res}(C_4, C_5, z) \equiv (x + \overline{y})$.

$C_{10}$ in combination with the unit clause $C_9$ yields $\overline{y} \oplus 0$. Under this assignment, the clause $C_6$ is unit, forcing us to assign 0 to $z$, which conflicts with clause $C_7$. Note that we obtained this conflict without making any decisions, i.e., we found a conflict at decision level zero. Accordingly, the formula is unsatisfiable.

**Exercise 8** Use the approach described in Section 3.6 to construct a resolution refutation proof for the formula presented in Exercise 7.

**Solution** The solution to this exercise follows the steps of the solution to Exercise 7 and is left to the reader.

**Exercise 9** Find an unsatisfiable core of the formula

$$(y) \cdot (x + \overline{y} + z) \cdot (\overline{x} + z) \cdot (x + \overline{y}) \cdot (\overline{x} + \overline{y}) .$$

(You are not allowed to provide the set of all clauses as a solution.) Is your solution minimal?
Solution  The set of clauses

\{ (y), (x + \overline{y} + z), (\overline{x} + z), (\overline{x} + \overline{y}) \}

forms a core of the formula in Exercise 9. This can be verified by means of resolution:

\[
\begin{align*}
\text{Res}((y), (x + \overline{y} + z), y) & \equiv (x + z) \\
\text{Res}((x + z), (\overline{x} + z), x) & \equiv (z) \\
\text{Res}((z), (\overline{x} + \overline{y}), z) & \equiv (\overline{y}) \\
\text{Res}((\overline{y}), (y), y) & = \square
\end{align*}
\]

Moreover, the core is minimal, since removing any one of the clauses “breaks” the core. Note that \{ (y), (x + \overline{y} + z), (\overline{x} + \overline{y}), (\overline{x} + \overline{y}) \} is an alternative minimal solution.

Exercise 10  Simplify the following formula using the substitution approach described in Section 3.10:

\[
\begin{align*}
w \cdot (\overline{q} + z) \cdot (\overline{q} + x) \cdot (\overline{x} + q) \cdot (\overline{p} + \overline{z}) \cdot (\overline{p} + \overline{x}) \cdot (z + x + p) \cdot \\
(\overline{p} + u) \cdot (\overline{q} + u) \cdot (\overline{v} + p + q) \cdot (\overline{y} + v) \cdot (\overline{u} + v) \cdot (\overline{v} + y + u) \cdot \\
(\overline{x} + w) \cdot (\overline{v} + w) \cdot (\overline{v} + x + v)
\end{align*}
\]

Solution  Note that we do not know which clauses are “definitional” (i.e., introduce functionally dependent variables). In practice, this information is often not available and inferring it is computationally prohibitively expensive. Therefore we will not attempt to do so. Instead, we start by dividing the clauses into sets according to the positive and negative occurrences of the literals as follows:
\( S_x = \{(\overline{q} + x), (z + x + p), (\overline{w} + x + v)\} \)

\( S_{\overline{x}} = \{ (\overline{z} + p), (\overline{p} + \overline{w}) \} \)

\( S_y = \{(\overline{v} + y + u)\} \)

\( S_{\overline{y}} = \{(\overline{y} + v)\} \)

\( S_z = \{(z + x + p)\} \)

\( S_{\overline{z}} = \{(\overline{z} + q), (\overline{p} + \overline{z})\} \)

\( S_p = \{(z + x + p), (\overline{p} + p + q)\} \)

\( S_q = \{(\overline{v} + \overline{x}), (\overline{p} + \overline{x})\} \)

\( S_u = \{(\overline{y} + q), (\overline{p} + u)\} \)

\( S_{\overline{u}} = \{(\overline{y} + u), (\overline{v} + u)\} \)

\( S_v = \{(\overline{v} + p + q), (\overline{v} + v)\} \)

\( S_{\overline{v}} = \{(\overline{v} + y + u), (\overline{v} + w)\} \)

\( S_w = \{(w), (\overline{v} + w)\} \)

\( S_{\overline{w}} = \{(\overline{v} + x + v)\} \)

Then, for each pair of sets \( S_\ell, S_{\overline{\ell}} \), we derive all possible resolvents and drop the resulting tautologies. If the resulting set of clauses \( \text{Res}(S_\ell, S_{\overline{\ell}}, \ell) \) is smaller than \( S_\ell \cup S_{\overline{\ell}} \), we replace the clauses \( S_\ell \cup S_{\overline{\ell}} \) with \( \text{Res}(S_\ell, S_{\overline{\ell}}, \ell) \). Otherwise, we retain the clauses \( S_\ell \cup S_{\overline{\ell}} \). The set of resolvents of \( S_x \) and \( S_{\overline{x}} \) has five elements:

\[
\text{Res}(S_x, S_{\overline{x}}, x) = \{(\overline{y} + p), (\overline{y} + w), (z + p + w), (\overline{w} + \overline{v} + p + q), (\overline{w} + \overline{p} + v)\}
\]

This is one clause less than \( S_x \cup S_{\overline{x}} \). Accordingly, replacing the clauses \( S_x \cup S_{\overline{x}} \) with the corresponding set of resolvents reduces the size of the formula. This strategy is implemented in the SAT-solver MINISAT [ES04,EB05].

**Exercise 11** Use the core-guided algorithm presented in Section 4.4.2 to determine the solution of the partial MAX-SAT problem

\[
(\overline{x} + \overline{y}) \cdot (x + z) \cdot (x + \overline{v}) \cdot (\overline{y} + u) \cdot (\overline{y} + \overline{w}) \cdot (x) \cdot (y),
\]

where only the clauses \((x)\) and \((y)\) may be dropped.

**Solution** Assume that the first unsatisfiable core we obtain is \((\overline{x} + \overline{y}, (x), (y))\). Accordingly, we augment the clauses \((x)\) and \((y)\) with relaxation variables and introduce a cardinality constraint which guarantees that at most one of these clauses is dropped:

\[
(\overline{x} + \overline{y}) \cdot (x + z) \cdot (x + \overline{v}) \cdot (\overline{y} + u) \cdot (\overline{y} + \overline{w}) \cdot (r + x) \cdot (s + y) \cdot \sum (r, s) \leq 1
\]
As illustrated in Figure 15, we can encode the constraint \( \sum (r,s) \leq 1 \) as \( (\overline{r} + \overline{s}) \), and we obtain the instance

\[
(\overline{x} + \overline{y}) \cdot (\overline{x} + z) \cdot (\overline{x} + \overline{y}) \cdot (\overline{y} + u) \cdot (\overline{y} + \overline{u}) \cdot (r + x) \cdot (s + y) \cdot (\overline{r} + \overline{s}),
\]

which is still unsatisfiable, since

\[
\text{Res}((\overline{x} + z), (\overline{x} + \overline{y}), z) = (\overline{x})
\]
\[
\text{Res}((\overline{y} + u), (\overline{y} + \overline{u}), u) = (\overline{y})
\]
\[
\text{Res}((r + x), (\overline{r} + \overline{s}), r) = (\overline{s} + x)
\]
\[
\text{Res}((s + y), (\overline{r} + \overline{s}), s) = (x + y)
\]
\[
\text{Res}((\overline{y}), (x + y), y) = (x)
\]
\[
\text{Res}((\overline{x}), (x), x) = \square
\]

Accordingly, we add additional relaxation variables to the clauses \((r+x)\) and \((s+y)\) in the next iteration of the algorithm in Figure 16 and obtain

\[
(\overline{x} + \overline{y}) \cdot (\overline{x} + z) \cdot (\overline{x} + \overline{y}) \cdot (\overline{y} + u) \cdot (\overline{y} + \overline{u}) \cdot (t + r + x) \cdot (v + s + y) \cdot (\overline{r} + \overline{s}) \cdot (\overline{t} + \overline{v})
\]

\[
\text{cardinality constraints}
\]

It is now possible for the satisfiability solver to relax both clauses \((r)\) and \((y)\) by choosing the assignment \(\{t \mapsto 1, r \mapsto 0, v \mapsto 0, s \mapsto 1\}\), for instance. Accordingly, the algorithm in Figure 16 reports that two clauses need to be dropped to make the formula satisfiable.

**Exercise 12** Use the algorithm presented in Section 4.5 to derive all minimal correction sets for the unsatisfiable formula

\[
\frac{C_1}{(x)} \cdot \frac{C_2}{(\overline{x})} \cdot \frac{C_3}{(\overline{x} + y)} \cdot \frac{C_4}{(\overline{y})} \cdot \frac{C_5}{(\overline{x} + z)} \cdot \frac{C_6}{(\overline{x})}.
\]

**Solution** (This example is presented in [LS08].) Due to the prioritisation of unit clauses, the first unsatisfiable core reported by the satisfiability checker is \(UC_1 = \{(x), (\overline{x})\}\). By adding relaxation variables to all clauses of this core and by constraining the respective relaxation literals, we obtain the formula

\[
(r_1 + x) \cdot (r_2 + \overline{x}) \cdot (\overline{x} + y) \cdot (\overline{y}) \cdot (\overline{x} + z) \cdot (\overline{x}) \cdot (\overline{r_1} + \overline{r_2})
\]

Since dropping the clause \((\overline{x})\) does not yield a satisfiable instance, the AllSAT procedure returns \(C_1\) as the only MCS of size one. Accordingly, we block the corresponding assignment by adding the blocking clause \((\overline{x})\):

\[
(r_1 + x) \cdot (r_2 + \overline{x}) \cdot (\overline{x} + y) \cdot (\overline{y}) \cdot (\overline{x} + z) \cdot (\overline{x}) \cdot (\overline{r_1} + \overline{r_2}) \cdot (\overline{x})
\]

and obtain a new core \(\{(\overline{x}), (r_1 + x), (\overline{x} + y), (\overline{y})\}\). Accordingly, \(UC_2 = \{C_1, C_2\} \cup \{C_1, C_3, C_4\}\), and we obtain the instrumented formula
\[(r_1 + x) \cdot (r_2 + \overline{x}) \cdot (r_3 + \overline{x} + y) \cdot (r_4 + \overline{y}) \cdot (\overline{x} + z) \cdot (r_1) \cdot \sum(r_1, r_2, r_3, r_4) \leq 2\]

The ALLSAT algorithm determines all minimal correction sets for this formula. Note that the clause \((r_1)\) prevents that the algorithm rediscovers the MCS \(\{C_1\}\) in this step. Since \(\text{Res}(\overline{r_1}, (r_1 + x)) \equiv (x)\), blocking \(C_1\) yields the formula

\[(x) \cdot (r_2 + \overline{x}) \cdot (r_3 + \overline{x} + y) \cdot (r_4 + \overline{y}) \cdot (\overline{x} + z) \cdot (r_1) \cdot \sum(r_1, r_2, r_3, r_4) \leq 2,\]

which is unsatisfiable. We obtain the new core \(\{C_1, C_5, C_6\}\) and execute the third iteration of the algorithm with \(\text{UC}_3 = \{C_1, C_2, C_3, C_4\} \cup \{C_1, C_5, C_6\}\). The corresponding instrumented and constrained version of the original formula is

\[(r_1 + x) \cdot (r_2 + \overline{x}) \cdot (r_3 + \overline{x} + y) \cdot (r_4 + \overline{y}) \cdot (\overline{x} + z) \cdot (r_5 + \overline{x}) \cdot (r_6) \cdot \sum(r_1, r_2, r_3, r_4, r_5, r_6) \leq 3\]

In this iteration, we obtain the MCSes \(\{C_2, C_3, C_5\}\), \(\{C_2, C_3, C_6\}\), \(\{C_2, C_4, C_5\}\), and \(\{C_2, C_3, C_6\}\). Adding the corresponding blocking clauses to \(\text{INSTRUMENT}(F)\) results in an unsatisfiable instance and the algorithm terminates.

**Exercise 13** Derive all minimal unsatisfiable cores for the formula presented in Exercise 12.

**Solution**  The set of MCSes for the formula in Exercise 12 is

\[
\{\{C_1\}, \{C_2, C_3, C_5\}, \{C_2, C_3, C_6\}, \{C_2, C_4, C_5\}, \{C_2, C_3, C_6\}\}.
\]

We construct the corresponding minimal hitting sets as follows:

<table>
<thead>
<tr>
<th>MCSes(F)</th>
<th>(C_1)</th>
<th>(C_2)</th>
<th>(C_3)</th>
<th>(C_4)</th>
<th>(C_5)</th>
<th>(C_6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>({C_1})</td>
<td>(\times)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>({C_2, C_3, C_5})</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>({C_2, C_3, C_6})</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>({C_2, C_4, C_5})</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>({C_2, C_3, C_6})</td>
<td>(\times)</td>
<td>(\times)</td>
<td>(\times)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hitting sets: \(\{C_1, C_2\}, \{C_1, C_3, C_4\}, \{C_1, C_5, C_6\}\)

**References**


[GGAP04] M. K. Ganai, A. Gupta, and P. Ashar. Efficient SAT-based Unbounded Symbolic Model Check-


