Notes on Validated Model Counting
Version of May 11, 2022

Randal E. Bryant

Computer Science Department
Carnegie Mellon University, Pittsburgh, PA, United States

1 Notation

Let $X = \{x_1, x_2, \ldots, x_n\}$ be a set of Boolean variables. An *assignment* is a function α assigning Boolean values to the variables: $\alpha : X \rightarrow \{0, 1\}$. We can also view an assignment as a set of *literals* $\{l_1, l_2, \ldots, l_n\}$, where each literal l_i is either x_i or $\overline{x}_i$, corresponding to the assignments $\alpha(x_i)$ = 1 or 0, respectively. We denote the set of all assignments over these variables as $\mathcal{U}$.

1.1 Boolean Functions

A *Boolean function* $f : 2^X \rightarrow \{0, 1\}$ can be characterized by the set of assignments for which the function evaluates to 1: $\mathcal{M}(f) = \{\alpha | f(\alpha) = 1\}$. Let **1** denote the Boolean function that assigns value 1 to every assignment, and **0** denote the assignment that assigns value 0 to every assignment. These are characterized by the universal assignment set $\mathcal{U}$ and the empty assignment set $\emptyset$, respectively.

From this we can define the *negation* of function f as the function $\neg f$ such that $\mathcal{M}(\neg f) = \mathcal{U} - \mathcal{M}(f)$. We can also define the conjunction and disjunction operations over functions f_1 and f_2 as characterized by the sets $\mathcal{M}(f_1 \wedge f_2) = \mathcal{M}(f_1) \cap \mathcal{M}(f_2)$ and $\mathcal{M}(f_1 \vee f_2) = \mathcal{M}(f_1) \cup \mathcal{M}(f_2)$.

For assignment α and a Boolean formula ϕ over X, we use the notation $\alpha[\phi/x_i]$ to denote the assignment α', such that $\alpha'(x_j) = \alpha(x_j)$ for all $j \neq i$ and $\alpha'(x_i) = \alpha(\phi)$, where $\alpha(\phi)$ is the value obtained by evaluating formula E with each variable assigned the value given by α. In particular, the notation $\alpha([\overline{x}_i/x_i])$ indicates the assignment in which the value assigned to x_i is negated, while others remain unchanged.

A Boolean function f is said to be *independent* of variable x_i if every $\alpha \in \mathcal{M}(f)$ has $\alpha([\overline{x}_i/x_i]) \in \mathcal{M}(f)$. The *dependency set* of f, denoted $D(f)$ consists of all variables x_i for which f is *not* independent.

1.2 Separable Cost Functions

Let $\mathcal{Z}$ denote the elements of a commutative ring. A *separable cost function* $\sigma : X \rightarrow \mathcal{Z}$ assigns a value from the ring to each variable. We extend this function by defining the cost of literal $\overline{x}_i$ as $\sigma(\overline{x}_i) = 1 - \sigma(x_i)$, the cost of an assignment as $\sigma(\alpha) = \prod_{l_i \in \alpha} \sigma(l_i)$, and the cost of a function f as $\sigma(f) = \sum_{\alpha \in \mathcal{M}(f)} \sigma(\alpha)$.

For ring elemement a, we use the notation $\sim\!a$ to denote $1 - a$.

Example 1: Let $\mathcal{Z}$ be the set of rational numbers of the form $a \cdot 2^b$ where a and b are integers. Let $\sigma(x_i) = 1/2$ for all variables x_i. The cost of every assignment is then $1/2^n$, and the cost of a function is its *density*, denoted $\rho(f)$. That is, the density of f, for which $0 \leq \rho(f) \leq 1$, is the fraction of assignments for which f evaluates to 1, with $\rho(\mathbf{0}) = 0$ and $\rho(\mathbf{1}) = 1$. The density of a function f can be scaled by 2^n to compute the total number of models $|\mathcal{M}(f)|$. This is the core task of model counting. Using density as the metric, rather than the number of models, has the advantage that it does not vary when the function is embedded in a larger domain $X' \supseteq X$.

Example 2: Let $\mathcal{Z}$ be the set of rational numbers. Assign a *weight* w_i to each variable x_i such that $0 \leq w_i \leq 1$ and let $\sigma(x_i) = w_i$. This implements *weighted model counting* under the restrictions that: 1) the weight of an assignment equals the product of the weights of its literals, and 2) the weight of a variable x_i and its negation $\overline{x}_i$ sum to 1.

Example 3: Let $\mathcal{Z}$ be a finite field with $z = |\mathcal{Z}| \geq 2n$, and let $\mathcal{H}$ be the set of functions mapping elements of X to elements of $\mathcal{Z}$. For two distinct functions f_1 and f_2 and a randomly chosen $h \in \mathcal{H}$, the probability that $h(f_1) \neq h(f_2)$ will be at least $\left(1 - \frac{1}{z}\right)^n \geq \left(1 - \frac{1}{2n}\right)^n > 1/2$. Therefore, these functions can be used as part of a randomized algorithm for equivalence testing [1].

1.3 Computing Cost Functions

Three key properties of separable cost functions make it possible, in some cases, to compute the cost of a Boolean formula without enumerating all of its satisfying solutions.

Proposition 1 (Negation). *For separable cost function σ and Boolean function f: $\sigma(\neg f) = 1 - \sigma(f) = \sim\!\sigma(f)$.*

Proposition 2 (Variable-Partitioned Conjunction). *For separable cost function σ and Boolean functions f_1 and f_2 such that $D(f_1) \cap D(f_2) = \emptyset$: $\sigma(f_1 \land f_2) = \sigma(f_1) \cdot \sigma(f_2)$.*

We use the notation $f_1 \land_{\mathsf{v}} f_2$ to denote the conjunction of f_1 and f_2 under the condition that f_1 and f_2 are defined over disjoint sets of variables.

Proposition 3 (Assignment-Partitioned Disjunction). *For separable cost function σ and Boolean functions f_1 and f_2 such that $\mathcal{M}(f_1) \cap \mathcal{M}(f_2) = \emptyset$: $\sigma(f_1 \lor f_2) = \sigma(f_1) + \sigma(f_2)$.*

We use the notation $f_1 \lor_{\mathsf{a}} f_2$ to denote the disjunction of f_1 and f_2 under the condition that f_1 and f_2 hold for mutually exclusive assignments.

2 Separable Schemas

Computing the cost function for a Boolean formula becomes straightforward when the formula contains only the operations $\land_{\mathsf{v}}$, $\lor_{\mathsf{a}}$, and $\neg$, as is demonstrated by Propositions 1–3. We define *separable schemas* as a direct-acyclic graph representation of such formulas. Representing formulas as a graph enables sharing subformulas, yielding a more compact representation.

2.1 Schema Definition

Table 1. Recursive Definition of Separable Schemas

S	Restrictions	$D(S)$	$\mathcal{M}(S)$
0	None	$\emptyset$	$\emptyset$
1	None	$\emptyset$	$\mathcal{U}$
x_i	None	$\{x_i\}$	$\{\alpha \mid \alpha(x_i) = 1\}$
$\neg S_1$	None	$D(S_1)$	$\mathcal{U} - \mathcal{M}(S_1)$
$S_1 \wedge_{\mathsf{v}} S_2$	$D(S_1) \cap D(S_2) = \emptyset$	$D(S_1) \cup D(S_2)$	$\mathcal{M}(S_1) \cap \mathcal{M}(S_2)$
$S_1 \vee_{\mathsf{a}} S_2$	$\mathcal{M}(S_1) \cap \mathcal{M}(S_2) = \emptyset$	$D(S_1) \cup D(S_2)$	$\mathcal{M}(S_1) \cup \mathcal{M}(S_2)$

The set of schemas over a set of variables $\{x_1, x_2, \ldots, x_n\}$ can be defined recursively, as is shown in Table 1. Each schema S has an associated dependency set $D(S)$ and an associated set of models $\mathcal{M}(S)$.

A key property of a Boolean formula represented by separable schema S is that, for any separable cost function σ, the cost of the formula $\sigma(S)$ can be computed with a linear number of ring operations.

2.2 Schema Normalization

Table 2. Normalization Rules

$\neg 0$	$\rightarrow$	1	$\neg 1$	$\rightarrow$	0
$\neg\neg S$	$\rightarrow$	S			
$S \wedge_{\mathsf{v}} 0$	$\rightarrow$	0	$0 \wedge_{\mathsf{v}} S$	$\rightarrow$	0
$S \wedge_{\mathsf{v}} 1$	$\rightarrow$	S	$1 \wedge_{\mathsf{v}} S$	$\rightarrow$	S
$S \vee_{\mathsf{a}} 0$	$\rightarrow$	S	$0 \vee_{\mathsf{a}} S$	$\rightarrow$	S
$S \vee_{\mathsf{a}} 1$	$\rightarrow$	1	$1 \vee_{\mathsf{a}} S$	$\rightarrow$	1

Table 2 shows a list of *normalizing* transformations to simplify a separable schema. These eliminate extra negations and remove constant terms, such that constants only occur in schemas when representing constant functions **0** and **1**.

2.3 Encoding the ITE Operation

The if-then-else (ITE) operation arises when converting the CNF representation of a formula into a separable schema, both for bottom-up approaches based on decision diagrams, and for top-down approaches based on CDCL. For functions f_1, f_2, and f_3, we define $\mathit{ITE}(f_1, f_2, f_3) = (f_1 \wedge f_2) \vee (\neg f_1 \wedge f_3)$. Observe that the $\vee$ operation in this expression satisfies the requirements for $\vee_{\mathsf{a}}$, since the first argument can only yield 1 for assignments that yield 1 for f_1, while the second can only yield 1 for assignments that yield 0 for f_1. Therefore, the only condition imposed on an expansion of *ITE* into the allowed schema operations is that the dependency set for f_1 must be disjoint from those of f_2 and f_3.

Table 3. Encodings of the ITE Operation

ITE Form	Encoding
$\mathit{ITE}(S_1, S_2, S_3)$	$(S_1 \wedge_{\mathsf{v}} S_2) \vee_{\mathsf{a}} (\neg S_1 \wedge S_3)$
$\mathit{ITE}(1, S_2, S_3)$	S_2
$\mathit{ITE}(0, S_2, S_3)$	S_3
$\mathit{ITE}(S_1, 1, 0)$	S_1
$\mathit{ITE}(S_1, 0, 1)$	$\neg S_1$
$\mathit{ITE}(S_1, S_2, 0)$	$S_1 \wedge_{\mathsf{v}} S_2$
$\mathit{ITE}(S_1, 0, S_3)$	$\neg S_1 \wedge_{\mathsf{v}} S_3$
$\mathit{ITE}(S_1, 1, S_3)$	$\neg(\neg S_1 \wedge_{\mathsf{v}} \neg S_3)$
$\mathit{ITE}(S_1, S_2, 1)$	$\neg(S_1 \wedge_{\mathsf{v}} \neg S_2)$

Table 3 shows different ways to encode an ITE operation into schema operations. All of these require the dependency set of the argument S_1 to be disjoint from those of arguments S_2 and S_3. The first row shows the most general case, requiring one $\vee_{\mathsf{a}}$ and two $\wedge_{\mathsf{v}}$ operations. The other rows show special cases, where one or more argument is a constant. Of these, the final two rows are particularly noteworthy. They make use of DeMorgan's Laws to convert disjunctions into conjunctions. In particular, for Boolean functions f_1 and f_2, we can write $\mathit{ITE}(f_1, 1, f_2)$ as $f_1 \vee f_2$, and by DeMorgan's Laws as $\neg(\neg f_1 \wedge \neg f_2)$. Similarly $\mathit{ITE}(f_1, f_2, 1) = \neg f_1 \vee f_2 = \neg(f_1 \wedge \neg f_2)$. These conjunctions can then be encoded with $\wedge_{\mathsf{v}}$ operations, since their arguments will have disjoint dependency sets.

3 Proof Framework for Cost Functions

The CRAT clausal proof framework provides a means to express a checkable proof that a Boolean formula, given in conjunctive normal form, is logically equivalent to a separable schema. Once this equivalence has been established, the schema can form the basis for computations enabled by the representation, including trusted model counting

The CRAT format draws its inspiration from the LRAT format for Boolean formulas and the QRAT format for quantified Boolean formulas (QBF). The following are its key properties:

- In addition to explicit clause additions and deletions, the proof contains declarations of $\wedge_{\mathsf{v}}$ and $\vee_{\mathsf{a}}$ operations.

    - These declarations implicitly add extension variables and their defining clauses to the proof. This is the only means for generating extension variables or adding blocked clauses to the proof.
    - The checker tracks the dependency set for every input and extension variable. When an extension variable is introduced based on the $\wedge_{\mathsf{v}}$ operation, the dependency sets of its arguments must be disjoint. The resulting extension variable has a dependency set equal to the union of those of its arguments.
    - Declaring a $\vee_{\mathsf{a}}$ operation requires a sequence of clauses providing a RUP proof that the arguments are mutually exclusive. This sequence can either be provided explicitly or inferred by the proof checker.
    - Boolean complement is provided implicitly by allowing the arguments of the $\vee_{\mathsf{a}}$ and $\wedge_{\mathsf{v}}$ operations to be literals and not just variables.
  - Clauses can also be added when they satisfy the RUP property, with respect to a sequence of existing clauses. This sequence can be either supplied explicitly or inferred by the proof checker.
  - Deleting clauses requires proving that the resulting formula is not weaker.
    - For an input clause or a clause declared by RUP addition, its deletion must be accompanied by a sequence of remaining clauses providing a RUP proof of the clause. This sequence can either be provided explicitly or inferred by the proof checker.
    - The clauses defining a $\wedge_{\mathsf{v}}$ or $\vee_{\mathsf{a}}$ operation are implicitly deleted by deleting the operation. This can only be done when the only undeleted clauses containing references to the associated extension variable are those implicitly defined when the operation was declared. This implies that there can be no undeleted operations having the operation result as an argument.

3.1 Syntax

Table 4. CRAT Step Types. C: clause identifier, L: literal, V: variable

Rule				Description
C	`i`	L^* `0`		Input clause
C	`a`	L^* `0`	C^+ `0`	Add RUP clause. Explicit hint
C	`a`	L^* `0`	`* 0`	Add RUP clause. Inferred hint
	`d`	C	C^+ `0`	Delete RUP clause. Explicit hint
	`d`	C	`* 0`	Delete RUP clause. Inferred hint
C	`p`	$V\ L\ L$		Declare $\wedge_{\mathsf{v}}$ operation
C	`s`	$V\ L\ L$	C^+ `0`	Declare $\vee_{\mathsf{a}}$ operation. Explicit hint
C	`s`	$V\ L\ L$	`* 0`	Declare $\vee_{\mathsf{a}}$ operation. Inferred hint

Table 4 shows the set of proof rules for the CRAT format. As with other clausal proof formats, a variable is represented by a positive integer v, with the first ones being input variables and successive ones being extension variables. Literal l is represented by a signed integer, with $-v$ being the complement of variable v. Each clause is indicated by a positive integer identifier C, with the first ones being the IDs of the input clauses and successive ones being the IDs of added clauses. Clause identifiers must be totally ordered, such that clause C can only reference clauses C' such that $C' < C$. Clause identifiers need not be consecutive.

The first set of proof rules are similar to those in other clausal proofs. Our syntax optionally allows input clauses to be listed with a rule of type `i`. Clauses can be added via RUP addition (command `a`), with the sequence of antecedent clauses (the "hint") either provided explicitly or to be inferred (indicated by the character '$\star$') by the proof checker. Similarly for clause deletion (command `d`).

The declaration of a $\wedge_{\mathsf{v}}$ operation has the form:

$$i \quad \mathtt{p} \quad v \quad l_1 \quad l_2$$

where i is a new clause ID, v is a positive integer that does not correspond to any previous variable, and l_1 and l_2 are signed integers representing literals of existing variables. This declaration implicitly causes three clauses to be added to the proof:

ID	Clause
i	$v\ -l_1\ -l_2$
$i{+}1$	$-v\ \ l_1$
$i{+}2$	$-v\ \ l_2$

The dependency sets for the arguments represented by literals l_1 and l_2 must be disjoint.

The declaration of a $\vee_{\mathsf{a}}$ operation has the form:

$$i \quad \mathtt{s} \quad v \quad l_1 \quad l_2 \quad H \quad \mathtt{0}$$

where i is a new clause ID, v is a positive integer that does not correspond to any previous variable, and l_1 and l_2 are signed integers representing literals of existing variables. Hint H can consist either of the single character $\star$, or it can be a sequence of clause IDs.

This declaration implicitly causes three clauses to be added to the proof:

ID	Clause
i	$-v\ \ l_1\ \ l_2$
$i{+}1$	$v\ -l_1$
$i{+}2$	$v\ -l_2$

The explicit or implied hints must provide a RUP proof of the clause $-l_1 \vee -l_2$.

3.2 Semantics

A CRAT proof follows the same general form as a QRAT dual proof [3]—one that ensures that each clause addition and each clause deletion preserves equivalence. With CRAT, however, clauses are defined both explicitly and implicitly. Starting with the set of input clauses, the proof consists of a sequence of steps that both add and delete clauses. Each addition must be truth preserving and each deletion must be falsehood preserving. At the end, all input clauses must have been deleted, and among the remaining clauses there must be only a single unit clause consisting of some variable or its complement. Except for trivial cases, the final literal will be an extension variable or its complement. That literal will indicate the root of the schema as the (possibly negated) output of a schema operation. Working from that root backward, the schema can be extracted from the CRAT file.

3.3 Example 1

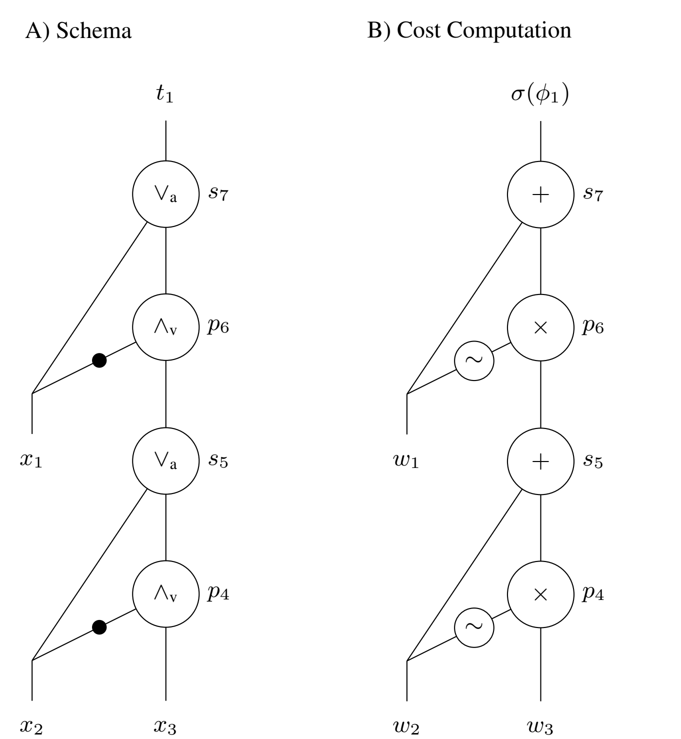

Fig. 1. Schema #1 for Formula $\phi_1 = x_1 \vee x_2 \vee x_3$ and its Cost Computation

As an illustration, consider the Boolean formula $\phi_1 = x_1 \vee x_2 \vee x_3$, represented by a single clause. We cannot directly use the $\vee_{\mathsf{a}}$ operation to form these disjunctions, since the sets of assignments satisfying the individual literals are not disjoint. Instead, we must decompose this formula into a sequence of operations. Figure 1A shows one such decomposition. The subscripts of the variables and the operator labels correspond to the numbers of the input and extension variables in the CRAT proof. Edges marked with dots indicate Boolean negation.

The conjunction of $\overline{x}_2$ and x_3 can be computed as $p_4 = \overline{x}_2 \wedge_{\mathsf{v}} x_3$, since the literals have disjoint dependency sets. We can then express the disjunction $x_2 \vee x_3$ as as $s_5 =$

A). CRAT File Contents

File line				Explanation
1	i	1 2 3 0		Input clause
2	p	4 -2 3		Declare $p_4 = \overline{x}_2 \wedge_{\mathsf{v}} x_3$
5	s	5 2 4	3 0	Declare $s_5 = x_2 \vee_{\mathsf{a}} p_4$
8	p	6 -1 5		Declare $p_6 = \overline{x}_1 \wedge_{\mathsf{v}} s_5$
11	s	7 1 6	9 0	Declare $s_7 = x_1 \vee_{\mathsf{a}} p_6$
14	a	7 0	12 13 7 6 2 1 0	Assert unit clause $[s_7]$
	d	1	4 5 10 11 14 0	Delete input clause

B). Proof Clauses

Clause				Explanation
1		1 2 3 0		Input clause
2		4 2 -3 0		Defining clauses for p_4
3		-4 -2 0		
4		-4 3 0		
		-2 -4 0	3 0	Mutual exclusion proof for s_5
5		-5 2 4 0		Defining clauses for s_5
6		5 -2 0		
7		5 -4 0		
8		6 1 -5 0		Defining clauses for p_6
9		-6 -1 0		
10		-6 5 0		
		-1 -6 0	9 0	Mutual exclusion proof for s_7
11		-7 1 6 0		Defining clauses for s_7
12		7 -1 0		
13		7 -6 0		
14		7 0	12 13 7 6 2 1 0	Assert unit clause $[s_7]$
	d	1	4 5 10 11 14 0	Delete input clause

Fig. 2. CRAT file #1 for formula $x_1 \vee x_2 \vee x_3$, and the resulting set of proof clauses

$x_2 \vee_{\mathsf{a}} p_4$. A similar process forms the disjunction $x_1 \vee x_2 \vee x_3$ by first forming the product $p_6 = \overline{x}_1 \wedge_{\mathsf{v}} s_5$ and the final sum $s_7 = x_1 \vee_{\mathsf{a}} p_6$.

The logical representation can readily be converted into a formula for computing $\sigma(\phi_1)$, the cost of formula ϕ_1, given a weight w_i for each variable x_i for $1 \leq i \leq 3$. This is illustrated in Figure 1B. Note how the Boolean negations become $\sim$ operations. This formula is valid for any cost function.

Figure 2A shows an annotated version of the CRAT file for this example, while 2B shows the sequence of clauses that constitute the proof, including those defined implicitly, and those required for mutual exclusion checks. Clause 1 is the input clause. Clauses 2–13 are added explcitly as the defining clauses for the four operations. Also shown are the required mutual exclusion proofs for the two sum operations. Proof clause 14 adds the unit clause for the extension variable s_7. We refer to the literal representing formula ϕ_1 as t_1, and we therefore have $t_1 = s_7$. The unit clause indicates that extension variable s_7 will evaluate to 1 for any assigment that satisfies the formula. We can write this as $\phi_1 \models t_1$. The deletion step at the end turns this around, showing that $t_1 \models \phi_1$, and therefore the input clause can be deleted, This completes a proof that t_1 is logically equivalent to the input formula.

3.4 Example 2A

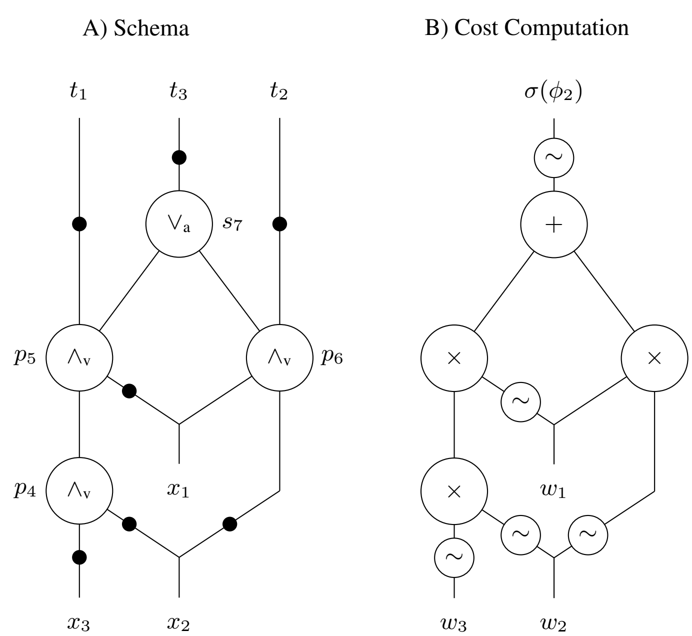

Fig. 3. Schema #2A for Formula $\phi_2 = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee x_2)$ and its Cost Computation

A). CRAT File Contents

Proof line				Explanation
1	i	1 2 3 0		Input clause C_1
2	i	-1 2 0		Input clause C_2
3	p	4 -2 3		Declare $p_4 = \overline{x}_2 \wedge_{\mathsf{v}} \overline{x}_3$
6	p	5 -1 4		Declare $p_5 = \overline{x}_1 \wedge_{\mathsf{v}} p_4 = \overline{x}_1 \wedge_{\mathsf{v}} \overline{x}_2 \wedge_{\mathsf{v}} \overline{x}_3$
9	a	-5 0	7 8 4 5 1 0	Assert $t_1 = \overline{p}_5 = x_1 \vee x_2 \vee x_3$
	d	1	3 6 7 0	Delete clause C_1
10	p	6 1 -2		Declare $p_6 = x_1 \wedge_{\mathsf{v}} \overline{x}_2$
13	a	-6 0	11 12 2 0	Assert $t_2 = \overline{p}_6 = \overline{x}_1 \vee x_2$
	d	2	10 13 0	Delete clause C_2
14	s	7 5 6	7 11 0	Declare $s_7 = \overline{t}_1 \vee_{\mathsf{a}} \overline{t}_2$
17	a	-7 0	9 13 0	Assert $t_3 = \overline{s}_7 = t_1 \wedge t_2$
	d	9	15 17 0	Delete t_1
	d	13	16 17 0	Delete t_2

B). Proof Clauses

Clause				Explanation
1		1 2 3 0		Input clause C_1
2		-1 2 0		Input clause C_2
3		4 2 3 0		Defining clauses for p_4
4		-4 -2 0		
5		-4 -3 0		
6		5 1 -4 0		Defining clauses for p_5
7		-5 -1 0		
8		-5 4 0		
9		-5 0	7 8 4 5 1 0	Assert $t_1 = \overline{p}_5 = x_1 \vee x_2 \vee x_3$
	d	1	3 6 7 0	Delete clause C_1
10		6 -1 2 0		Defining clauses for p_6
11		-6 1 0		
12		-6 -2 0		
13		-6 0	11 12 2 0	Assert $t_2 = \overline{p}_6 = \overline{x}_1 \vee x_2$
	d	2	10 13 0	Delete clause C_2
		-5 -6 0	7 11 0	Mutual exclusion proof for s_7
14		-7 5 6 0		Defining clauses for s_7
15		7 -5 0		
16		7 -6 0		
17		-7 0	9 13 0	Assert $t_3 = \overline{s}_7 = t_1 \wedge t_2$
	d	9	15 17 0	Delete t_1
	d	13	16 17 0	Delete t_2

Fig. 4. CRAT file #2A for formula $\phi_2 = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee x_2)$, and the resulting set of proof clauses

As a more complex example, consider the Boolean formula ϕ_2 given by the conjunction of clauses $C_1 = x_1 \vee x_2 \vee x_3$ and $C_2 = \overline{x}_1 \vee x_2$. With this example, we also demonstrate the use of DeMorgan's Laws to provide a more compact encoding of the formula, similar to the use of these laws when encoding ITE operations in Table 3.

Figure 3 shows a schema representing the formula, and Figure 4 shows the associated CRAT file and proof clauses. This proof was generated via a bottom-up strategy, such as would be created using BDDs. It creates schematic representations of the input clauses and then forms their conjunction. In the proof, unit clauses are generated for the representations of the input clauses, and then the input clauses are deleted. These intermediate unit clauses are used to justify a unit clause for the final root, and then they are deleted.

Using DeMorgan's Laws, C_1 can be written as $t_1 = \neg[\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3]$, and this can be expressed using $\wedge_{\mathsf{v}}$ operations s_4 and s_5, shown in Figure 3A. (Note that t_1 in this case is logically equivalent to root t_1 in the schema of Figure 1A, but the use of negation enables it to be represented with two operations rather than four.) Similarly, C_2 can be written as $t_2 = \neg[x_1 \wedge \overline{x}_2]$, and this can be represented by $\wedge_{\mathsf{v}}$ operation p_6. Terms t_1 and t_2 are asserted as unit clauses on proof lines 9 and 13, allowing the input clauses to be deleted. The conjunction $t_1 \wedge t_2$ can be written as $t_3 = \neg[\overline{t_1} \vee \overline{t_2}]$, represented by $\vee_{\mathsf{a}}$ operation s_7. Term t_3 is asserted as a unit clause on proof line 17. Based on this, the unit clauses for terms t_1 and t_2 can be deleted. Term t_3 then becomes the unique root of the cost computation shown in Figure 3B.

3.5 Example 2B

Figure 5 shows an alternate schema representing the same formula ϕ_2 as in Example 2A, and Figure 6 shows the associated CRAT proof. This proof was generated via a top-down strategy, such as would be created using a model counter based on CDCL. It starts by splitting on variable x_1. Clause C_1 is trivially satisfied when x_1 is assigned 1, and clause C_2 becomes the clause $C_2' = x_2$. On the other hand, clause C_2 is trivially satisfied when x_1 is assigned 0, and clause C_1 becomes $C_1' = x_2 \vee x_3$. Clause C_1' can be represented schematically as $\neg[\overline{x}_2 \wedge_{\mathsf{v}} \overline{x}_3]$, with this operation labeled p_4 in Figure 5A. The splitting on variable x_1 can be rejoined as *ITE*$(x_1, x_2, \overline{p_4})$, and this ITE operation can be expressed using the product operations p_5 and p_6, joined by the sum operation $t = s_7$.

The two schemas shown in Figures 3A and 5A have similar structure. They have very different negation patterns, but they are logically equivalent. Their associated cost computations (Figures 3B and 5B) also yield the same results for arbitrary weights w_1, w_2, and w_3.

The CRAT proof for the top-down approach follows a different pattern than does the proof based on a bottom-up construction. It does not create any intermediate unit clauses. Instead, it constructs a proof that the root $t = s_7$ holds as a unit clause by splitting into the two assignments for variable x_1. The proof that $\overline{x}_1 \rightarrow s_7$ (proof line 16) builds on the proof that $\overline{x}_1 \rightarrow \overline{p}_4$ (proof line 15), which derives from clause C_1. The proof that $x_1 \rightarrow x_7$ (proof line 17) derives from clause C_2. These two are combined to yield the unit clause s_7 (proof line 18). Given this unit clause, the two input clauses can then be deleted.

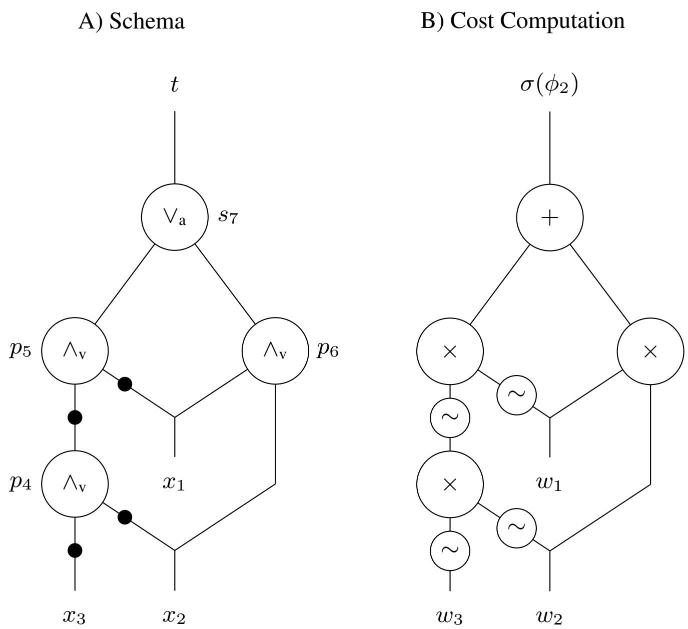

Fig. 5. Schema #2B for Formula $\phi_2 = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee x_2)$ and its Cost Computation

4 Looking Ahead

4.1 Implementing Certified Counters

Given an arbitrary CNF formula, we can use BDD operations to generate a schematic representation. The proof generation can follow the methods we have used for generating unsatisfiability proofs of Boolean formulas [4] and dual proofs of quantified Boolean formulas [3]. Each BDD node can be expressed as an ITE operation and make use of the encodings shown in Table 3.

A second class of model counters proceeds top-down, based on the CDCL framework. These choose a splitting variable x and recursively construct schemas S_1 and S_0 for the two assignments to the variable. These are combined as *ITE*(x, S_1, S_0), using one of the encodings of *ITE* shown in Table 3. Like CDCL, the top-down algorithm can make use of unit propagation, conflict detection, and clause learning. It can also make use of *variable* partitioning. That is, suppose for some partial assignment to the variables, the input clauses decompose into two or more sets over disjoint variables. Then the schema for each of these partitions can be generated separately, and these are joined via the $\wedge_{\mathsf{v}}$ operation.

4.2 TO-DO List

- Proof Framework
  - Generalities and details of the format

A). CRAT File Contents

File line				Explanation
1		1 2 3 0		Input clause C_1
2	i	-1 2 0		Input clause C_2
3	p	4 -2 3		Declare $p_4 = \overline{x}_2 \wedge_{\mathsf{v}} \overline{x}_3$
6	p	5 -1 -4		Declare $p_5 = \overline{x}_1 \wedge_{\mathsf{v}} \overline{p_4}$
9	p	6 1 2		Declare $p_6 = x_1 \wedge_{\mathsf{v}} x_2$
12	s	7 5 6	7 10 0	Declare $s_7 = p_5 \vee_{\mathsf{a}} p_6$
15	a	1 -4 0	4 5 1 0	Justify $\overline{x}_1 \rightarrow \overline{p_4}$
16	a	1 7 0	13 6 15 0	Justify $\overline{x}_1 \rightarrow s_7$
17	a	-1 7 0	14 9 2 0	Justify $x_1 \rightarrow s_7$
18	a	7 0	16 17 0	Justify unit clause $t = s_7$
	d	1	3 8 10 12 18 0	Delete C_1
	d	2	11 7 12 18 0	Delete C_2

B). Proof Clauses

File line				Explanation
1		1 2 3 0		Input clause C_1
2		-1 2 0		Input clause C_2
3		4 2 3 0		Defining clauses for p_4
4		-4 -2 0		
5		-4 -3 0		
6		5 1 4 0		Defining clauses for p_5
7		-5 -1 0		
8		-5 -4 0		
9		6 -1 -2 0		Defining clauses for p_6
10		-6 1 0		
11		-6 2 0		
		-5 -6	7 10 0	Mutual exclusion proof for s_7
12		-7 5 6 0		Defining clauses for s_7
13		7 -5 0		
14		7 -6 0		
15		1 -4 0	4 5 1 0	Justify $\overline{x}_1 \rightarrow \overline{p_4}$
16		1 7 0	13 6 15 0	Justify $\overline{x}_1 \rightarrow s_7$
17		-1 7 0	14 9 2 0	Justify $x_1 \rightarrow s_7$
18		7 0	16 17 0	Justify unit clause $t = s_7$
	d	1	3 8 10 12 18 0	Delete C_1
	d	2	11 7 12 18 0	Delete C_2

Fig. 6. CRAT file #2B for formula $\phi_2 = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee x_2)$, and the resulting set of proof clauses

    - Can some form of abstraction be incorporated?
      * Want to abstract a subformula to consider only on its cost and dependency set
      * Could represent with fresh extension variable
      * But how to prove logical equivalence?
- Checker
  - Working prototype
  - C/C++ (or Rust?)
  - Formally verified
- Counters
  - BDD-based
    * Prototype
    * C/C++
  - SDD-based
    * Bottom-up
    * Top-down
  - Others?

References

1. Blum, M., Chandra, A.K., Wegman, M.N.: Equivalence of free Boolean graphs can be decided probabilistically in polynomial time. Information Processing Letters **10**(2), 80–82 (18 March 1980)
2. Bryant, R.E.: Graph-based algorithms for Boolean function manipulation. IEEE Trans. Computers **35**(8), 677–691 (1986)
3. Bryant, R.E., Heule, M.J.H.: Dual proof generation for quantified Boolean formulas with a BDD-based solver. In: Conference on Automated Deduction (CADE). LNAI, vol. 12699, pp. 433–449 (2021)
4. Bryant, R.E., Heule, M.J.H.: Generating extended resolution proofs with a BDD-based SAT solver. In: Tools and Algorithms for the Construction and Analysis of Systems (TACAS) (2021)