Notes on
Pseudo-Boolean Implication Proofs
Version of October 5, 2023

Randal E. Bryant

Computer Science Department
Carnegie Mellon University, Pittsburgh, PA, United States
Randy.Bryant@cs.cmu.edu

This notes describes some ideas on converting unsatisfiability proofs for pseudo-Boolean (PB) constraints into clausal proofs based on the DRAT proof system.

1 Background

This section gives brief definitions of pseudo-Boolean constraints and their properties. A more extensive introduction is provided by Gocht in his PhD thesis [Gocht-Phd-2022].

Consider a set of Boolean variables X. For $x \in X$, *literal* ℓ can denote either x or its negation, written $\overline{x}$. We write $\overline{\ell}$ to denote $\overline{x}$ when $\ell = x$ and x_i when $\ell = \overline{x}$.

A *pseudo-Boolean constraint* is a linear expression, viewing Boolean variables as ranging over integer values 0 and 1. That is, a constraint C has the form

$$\sum_{1 \leq i \leq n} a_i \ell_i \quad \# \quad b \tag{1}$$

where: 1) the relational operator $\#$ is $<$, $\leq$, $=$, $\geq$, or $>$, and 2) the coefficients a_i, as well as the constant b, are integers. Constraints with relational operator $=$ are referred to as *equational constraints*, while others are referred to as *ordering constraints*.

Constraint C denotes a Boolean function, written $[\![C]\!]$, mapping assignments to the set of variables X to 1 (true) or 0 (false). Constraints C_1 and C_2 are said to *equivalent* when $[\![C_1]\!] = [\![C_2]\!]$. Constraint C is said to be *infeasible* when $[\![C]\!] = \bot$, i.e., it always evaluates 0. C is said to be *trivial* when $[\![C]\!] = \top$, i.e., it always evaluates to 1.

As described in [Gocht-Phd-2022], the following are some properties of pseudo-Boolean constraints:

- Constraints with relational operators $<$, $\leq$, and $>$ can be converted to equivalent constraints with relational operator $\geq$.
- The logical negation of an ordering constraint C, written $\overline{C}$, can also be expressed as a constraint. That is, assume that C has been converted to a form where it has relational operator $\geq$. Then replacing $\geq$ by $<$ yields the negation of C.
- A constraint C with relational operator $=$ can be converted to the pair of constraints $C_{\leq}$ and $C_{\geq}$, formed by replacing $\#$ in (1) by $\leq$ and $\geq$, respectively. These then satisfy $[\![C]\!] = [\![C_{\leq}]\!] \land [\![C_{\geq}]\!]$.

We will generally assume that constraints have relational operator $\geq$, since other forms can be translated to it. In some contexts, however, we will maintain equational constraints intact, to avoid replacing it by two ordering constraints.

We consider two *normalized forms* for ordering constraints: A *coefficient-normalized* constraint has only nonnegative coefficients. By convention, we require with this form that literal $\ell_i = x_i$ for any i such that $a_i = 0$. A *variable-normalized* constraint has only positive literals. Converting between the two forms is straightforward using the identity $\overline{x}_i = 1 - x_i$. In reasoning about PB constraints, the two forms can be used interchangeably. Typically, the coefficient-normalized form is more convenient when viewing a PB constraint as a logical expression, while the variable-normalized form is more convenient when viewing a constraint as an arithmetic expression. In this document, we focus on the logical aspects, giving the general form of constraint C as

$$\sum_{1 \leq i \leq n} a_i \ell_i \quad \geq \quad b \tag{2}$$

with each $a_i \geq 0$, and with $\ell_i = x_i$ whenever $a_i = 0$.

Ordering constraint C in coefficient-normalized form is trivial if and only if $b \leq 0$. Similarly, C is infeasible if and only if $b > \sum_{1 \leq i \leq n} a_i$. By contrast, testing feasibility or triviality of an equational constraint is not straightforward, in that an instance of the subset sum problem [Garey] can be directly encoded as an equational constraint.

An *assignment* is a mapping $\rho : X' \rightarrow \{0, 1\}$, for some $X' \subseteq X$. The assignment is *total* when $X' = X$ and *partial* when $X' \subset X$. Assignment ρ can also be viewed as a set of literals, where $x_i \in \rho$ when $\rho(x_i) = 1$ and $\overline{x}_i \in \rho$ when $\rho(x_i) = 0$.

Some nomenclature regarding constraints of the form of (2) will prove useful. The *constraint literals* are those literals ℓ_i such that $a_i \neq 0$. A *cardinality constraint* has $a_i \in \{0, 1\}$ for $1 \leq i \leq n$. A cardinality constraint with $b = 1$ is referred to as a *clause*: at least one of the constraint literals must be assigned 1 to satisfy the constraint. A cardinality constraint with $\sum_{1 \leq i \leq n} a_i = b$ is referred to as a *conjunction*: all of the constraint literals must be assigned 1 to satisfy the constraint. Observe that any assignment ρ can be viewed as a conjunction, having coefficient $a_i = 1$ for each $\ell_i \in \rho$. A conjunction with for which $a_i = 1$ for just a single value of i is referred to as a *unit* constraint: it is satisfied if and only if literal ℓ_i is assigned 1.

We let $C|_\rho$ denote the constraint resulting when C is simplified according assignment ρ. That is, assume ρ is defined over a set of variables X' and partition the indices i for $1 \leq i \leq n$ into three sets: I^+, consisting of those indices i such that $\ell_i \in \rho$, I^-, consisting of those indices i such that $\overline{\ell}_i \in \rho$, and I^X consisting of those indices i such that $x_i \notin X'$. With this, $C|_\rho$ can be written as $\sum_{1 \leq i \leq n} a'_i \;\; \geq \;\; b'$ with a'_i equal to a_i for $i \in I^X$ and equal to 0 otherwise, and with $b' = b - \sum_{i \in I^+} a_i$.

A pseudo-Boolean *formula* F is a set of pseudo-Boolean constraints. We say that F is *satisfiable* when there is some assignment ρ that satisfies all of the constraints in F, and *unsatisfiable* otherwise.

2 (Reverse) Unit Propagation

Consider constraint C in coefficient-normalized form. Literal ℓ is *unit propagated* by C when the assignment $\rho = \{\overline{\ell}\}$ causes the constraint $C|_\rho$ to become infeasible. As the name implies, a unit-propagated literal ℓ then becomes a unit constraint. Observe that a single constraint can unit propagate multiple literals. For example, $4x_1 + 3\overline{x}_2 + x_3 \geq 6$ unit propagates both x_1 and $\overline{x}_2$. For an ordering constraint C in coefficent-normalized form (2), detecting which literals unit propagate is straightforward. Let $A = \sum_{1 \leq i \leq n} a_i$. Then literal ℓ_i unit propagates if and only if $A - a_i < b$, i.e., $a_i > A - b$. For example, the constraint $4x_1 + 3\overline{x}_2 + x_3 \geq 6$ has $A = 7$ and $b = 6$, yielding $A - b = 1$. This justifies the unit propagations of both x_1 and $\overline{x}_2$.

For constraint C, we let $\mathit{Unit}(C)$ denote the set of literals it unit propagates. Often, by simplifying a constraint C according to a partial assignment ρ, the simplified constraint $C|_\rho$ will unit propagate new literals, given by $\mathit{Unit}(C|_\rho)$. These literals can then be added to the partial assignment. Formally, define the operation *Uprop* as $\mathit{Uprop}(\rho, C) = \rho \cup \mathit{Unit}(C|_\rho)$. *Unit propagation* is then the process of repeatedly applying this operation to a set of clauses to expand the set of literals in a partial assignment.

Consider a formula F consisting of a set of constraints $C_1, C_2, \ldots, C_m$. The *reverse unit propagation* (RUP) proof rule [Gocht-Phd-2022] uses unit propagation to prove that *target constraint* C can be added to a formula while preserving its set of satisfying assignments. That is, any assignment that satisfies F also satisfies $F \wedge C$. RUP justifies C by assuming $\overline{C}$ holds and showing, via a sequence of *RUP steps*, that this leads to a contradiction. It accumulates a partial assignment ρ based on unit propagations starting the empty set. Each RUP step accumulates more assigned literals by performing a unit propagation of the form $\rho \leftarrow \mathit{Uprop}(\rho, D)$, where constraint D is either C_j, a prior constraint, or $\overline{C}$, the negation of the target constraint. The final step causes a contradiction, where $D|_\rho$ is infeasbile.

2.1 RUP Example

As an example, consider the following three constraints:

ID	Constraint					
C_1	x_1	$+$	$2x_2$	$+$	$\overline{x}_3$	≥ 2
C_2	$\overline{x}_1$	$+$	$\overline{x}_2$	$+$	$2x_3$	≥ 2
C_3	x_1	$+$	$2\overline{x}_2$	$+$	$3\overline{x}_3$	≥ 3

Our goal is to add the constraint $C = 2x_1 + x_2 + x_3 \geq 2$. The RUP steps proceeds as follows:

1. We can see that $\overline{C} = 2\overline{x}_1 + \overline{x}_2 + \overline{x}_3 \geq 3$, and this unit propagates assignment $\rho_1 = \{\overline{x}_1\}$.
2. With this, constraint C_1 simplifies to $2x_2 + \overline{x}_3 \geq 2$, and this unit propagates x_2, giving $\rho_2 = \{\overline{x}_1, x_2\}$.
3. Constraint C_2 simplifies to $2x_3 \geq 1$, which unit propagates x_3, giving $\rho_3 = \{\overline{x}_1, x_2, x_3\}$.
4. Constraint C_3 simplifies to $0 \geq 3$, which is infeasible.

3 Pseudo-Boolean Implication Proofs

A Pseudo-Boolean Implication Proof (PBIP) provides a systematic way to prove that a PB formula F is unsatisfiable. It is given by a sequence of constraints, referred to as the *proof sequence*:

$$C_1, C_2, \ldots, C_m, C_{m+1}, \ldots, C_t$$

such that the first m constraints are those of formula F, while each *added* constraint C_i for $i > m$ follows by implication from the preceding constraints. That is,

$$\bigwedge_{1 \leq j < i} [\![C_j]\!] \quad \Rightarrow \quad [\![C_i]\!] \tag{3}$$

The proof completes with the addition of an infeasible constraint for C_t. By the transitivity of implication, we have therefore proved that F is not satisfiable.

Constraints C_i with $i > m$, can be added in two different ways, corresponding to two different reasoning modes.

1. In *implication mode*, constraint C_i follows by implication from at most two prior constraints in the proof sequence. That is, for some $H_i \subseteq \{C_1, C_2, \ldots, C_{i-1}\}$ with $|H_i| \leq 2$ such that:

$$\bigwedge_{C_j \in H_i} [\![C_j]\!] \quad \Rightarrow \quad [\![C_i]\!] \tag{4}$$

   Set H_i is referred to as the *hint* for proof step i.

2. In *RUP* mode, the new constraint is justified by reverse unit propagation. Again, a sequence of hints is specified, where each hint is of either of the form $[C_j, \ell]$, where $j \leq i$ and ℓ is the unit literal propagated by this step, or of the form $[C_j]$, where $j \leq i$. When $j < i$, unit propagation is performed using constraint C_j, while for $j = i$, it is performed using $\overline{C}_i$, the negation of the target constraint. The final hint is of the form $[C_j]$. Note that if a single constraint unit propagates multiple literal, these are listed as separate steps.

Unless $P = NP$, we cannot guarantee that a proof checker can validate even a single implication step of a PBIP proof in polynomial time. In particular, consider an equational constraint C encoding an instance of the subset sum problem, and let $C_{\leq}$ and $C_{\geq}$ denote its conversion into a pair of ordering constraints such that $[\![C]\!] = [\![C_{\leq}]\!] \wedge [\![C_{\geq}]\!]$. Consider a PBIP proof step to add the constraint $\overline{C}_{\leq}$ having the $C_{\geq}$ as the only hint. Proving that $[\![C_{\geq}]\!] \Rightarrow [\![\overline{C}_{\leq}]\!]$, requires proving that $[\![C_{\leq}]\!] \wedge [\![C_{\geq}]\!] = \bot$, i.e., that C is unsatisfiable.

On the other hand, checking the correctness of a PBIP proof can be performed in *pseudo-polynomial* time, meaning that the complexity will be bounded by a polynomially sized formula over the numeric values of the integer parameters. This can be done using binary decision diagrams [BBH-2022]. In particular, an ordering constraint over n variables in coefficient-normalized form with constant b will have a BDD representation with at most $b \cdot n$ nodes. For an implication proof step where the added constraints and the hints all have constants less than or equal to b, the number of BDD operations to validate the step will be $O(b^2 \cdot n)$ when there is a single hint and $O(b^3 \cdot n)$ when there are two hints. This complexity is polynomial in b, but it would be exponential in the size of a binary representation of b. The number of BDD operations for each unit propagation step in a RUP proof will be linear in the size of the BDD and therefore $O(b \cdot n)$.

4 Converting PBIP Proof into Clausal Proof

We convert PBIP proofs into clausal proofs in the LRAT format using *trusted* Binary Decision Diagrams, or TBDDs. TBDDs extend conventional BDDs by having their standard operations also generate proof steps. We denote BDDs by their root nodes, using bold letters, e.g., $\mathbf{u}$. A TBDD $\dot{\mathbf{u}}$ consists of the following:

- A BDD having root node $\mathbf{u}$
- A Boolean extension variable u along with an associated proof clauses defining the semantic relation between $\mathbf{u}$, the node variable x, and child nodes nodes $\mathbf{u}_1$ and $\mathbf{u}_0$

- A proof of the unit clause $[u]$ indicating that the BDD will evaluate to 1 for any assignment that satisfies the input formula

We assume our trusted BDD package implements the following operations

$\mathsf{BDD}(C)$: Generate a BDD representation of pseudo-Boolean constraint C

$\mathsf{BDD\_AND}(\mathbf{u}, \mathbf{v})$: Compute BDD $\mathbf{w}$ as the conjunction of BDDs $\mathbf{u}$ and $\mathbf{v}$. Also generate proof steps ending with the addition of the clause $[\overline{u} \vee \overline{v} \vee w]$ proving the $(u \wedge v) \Rightarrow w$.

$\mathsf{BDD\_IMPLY}(\mathbf{u}, \mathbf{v})$: Generate proof steps ending with the addition of the clause $[\overline{u} \vee v]$ indicating that $u \Rightarrow v$.

$\mathsf{BDD\_FALSIFIES}(\rho, \mathbf{u})$: For (possibly partial) assignment $\rho = \{\ell_1, \ell_2, \ldots, \ell_k\}$ generate proof steps ending with the addition of the clause $[\overline{\ell}_1 \vee \overline{\ell}_2 \vee \cdots \vee \overline{\ell}_k \vee \overline{u}]$. This clause indicates that any total assignment consistent with ρ will define a path in the BDD leading from root node $\mathbf{u}$ to the leaf node representing false.

$\mathsf{BDD\_SATISFIES}(\rho, \mathbf{u})$: For (possibly partial) assignment $\rho = \{\ell_1, \ell_2, \ldots, \ell_k\}$ generate proof steps ending with the addition of the clause $[\overline{\ell}_1 \vee \overline{\ell}_2 \vee \cdots \vee \overline{\ell}_k \vee u]$. This clause indicates that any total assignment consistent with ρ will define a path in the BDD leading from root node $\mathbf{u}$ to the leaf node representing true.

Our goal is the create a TBDD representation $\dot{\mathbf{u}}_i$ for each constraint C_i in the proof sequence. The final step will generate a trusted BDD for the BDD leaf node representing false. This will cause the empty clause to be added to the proof. When adding constraint C_i, its BDD representation $\mathbf{u}_i$ can be generated as $\mathsf{BDD}(C_i)$. To upgrade this to the trusted BDD $\dot{\mathbf{u}}_i$ requires generating the unit clause $[u_i]$. We assume that every prior proof constraint $C_{i'}$, with $i' < i$, has a TBDD representation $\dot{\mathbf{u}}_{i'}$ with an associated unit clause $[u_{i'}]$.

When C_i is added by implication mode, generating its unit clause is based on the constraints given as the hint. If the hint consists of the single constraint $C_{i'}$ we can make use of its TBDD representation $\dot{\mathbf{u}}_{i'}$, by performing the implication test $\mathsf{BDD\_IMPLY}(\mathbf{u}_{i'}, \mathbf{u}_i)$, generating the clause $[\overline{u}_{i'}, u_i]$. Resolving this with the unit clause $[u_{i'}]$ then gives the unit clause $[u_i]$. When the hint consists of two constraints $C_{i'}$ and $C_{i''}$, we can make use of their TBDD representation $\dot{\mathbf{u}}_{i'}$ and $\dot{\mathbf{u}}_{i''}$. That is, let $\mathbf{w} = \mathsf{BDD\_AND}(\mathbf{u}_{i'}, \mathbf{u}_{i''})$, generating the clause $[\overline{u}_{i'} \vee \overline{u}_{i''} \vee w]$, and then perform the implication test $\mathsf{BDD\_IMPLY}(w, \mathbf{u}_i)$, generating the clause $[\overline{w} \vee u_i]$. Resolving these clauses with the unit clauses for TBDDs $\dot{\mathbf{u}}_{i'}$ and $\dot{\mathbf{u}}_{i''}$ yields the unit clause $[u_i]$.

Adding constraint C_i via a sequence of RUP steps requires converting its proof by contradiction into a conventional implication proof. Let $\mathbf{u}_i$ denote the BDD representation of constraint C_i. For each literal ℓ that is unit propagated by a RUP step, we add the clause $[u_i \vee \ell]$, indicating that literal ℓ will hold if the target constraint is falsified. To do so for literal ℓ_k, suppose that we have clauses of the form $[u_i \vee \ell_j]$ for $1 \leq j \leq k$, and that unit propagation is based either on constraint $D = C_{i'}$ for $i' < i$, represented by TBDD node $\dot{\mathbf{u}}_{i'}$ and denoted by literal $u_{i'}$, or based on constraint $D = \overline{C}_i$ and denoted by literal $\overline{u}_i$.

Assignment $\rho = \{\ell_1, \ell_2, \ldots, \ell_{k-1}, \overline{\ell}_k\}$ should cause $D|_\rho$ to be infeasible. For $D = C_{i'}$, calling $\mathsf{BDD\_FALSIFIES}(\rho, \mathbf{u}_{i'})$ will generate the clause $[\overline{\ell}_1 \vee \overline{\ell}_2 \vee \cdots \vee \overline{\ell}_{k-1} \vee \ell_k \vee \overline{u}_{i'}]$. Resolving this with clauses of the form $[u_i \vee \ell_j]$ as well as the unit clause $[u_{i'}]$ will yield clause $[u_i \vee \ell_k]$. For $D = \overline{C}_i$, calling $\mathsf{BDD\_SATISFIES}(\rho, \mathbf{u}_i)$ will generate the clause $[\overline{\ell}_1 \vee \overline{\ell}_2 \vee \cdots \vee \overline{\ell}_{k-1} \vee \ell_k \vee u_i]$. Resolving this with clauses of the form $[u_i \vee \ell_j]$ will yield clause $[u_i \vee \ell_k]$. For the final step, no unit propagation occurs, and so the resolution steps will yield unit clause $[u_i]$, completing the validation of constraint C_i.