Decision Diagrams for Linear Arithmetic

Sagar Chaki  
SEI/CMU  
chaki@sei.cmu.edu

Arie Gurfinkel  
SEI/CMU  
arie@sei.cmu.edu

Ofer Strichman  
Technion  
ofers@ie.technion.ac.il

Abstract—Boolean manipulation and existential quantification of numeric variables from linear arithmetic (LA) formulas is at the core of many program analysis and software model checking techniques (e.g., predicate abstraction). We present a new data structure, Linear Decision Diagrams (LDDs), to represent formulas in LA and its fragments, which has certain properties that make it efficient for such tasks. LDDs can be seen as an extension of Difference Decision Diagrams (DDDs) to full LA. Beyond this extension, we make three key contributions. First, we extend sifting-based dynamic variable ordering (DVO) from BDDs to LDDs. Second, we develop, implement, and evaluate several algorithms for existential quantification. Third, we implement LDDs inside CUDD, a state-of-the-art BDD package, and evaluate them on a large benchmark consisting of 850 functions derived from the source code of 25 open source programs. Overall, our experiments indicate that LDDs are an effective data structure for program analysis tasks.

I. INTRODUCTION

Many program analysis problems — e.g., computation and application of predicate abstraction, image computation, function summarization — are ultimately reduced to manipulating propositional formulas over some theory. Typically, two types of operations are required: (i) Boolean (conjunction, negation, etc.) and (ii) existential quantification (henceforth QELIM). For example, the predicate abstraction of a transition relation \( R \) is computed as

\[
\exists \vec{x}, \vec{x}'. R(\vec{x}, \vec{x}') \land \left( \bigwedge_{i=1}^{n} v_i \leftrightarrow p_i(\vec{x}) \right) \land \left( \bigwedge_{i=1}^{n} v'_i \leftrightarrow p_i(\vec{x}') \right),
\]

where \( \vec{x}, \vec{x}' \) are current- and next-state propositional variables, \( v, v' \) are current- and next-state propositional abstract variables, and \( p_i \) is the definition of the \( i \)-th abstract variable in terms of \( \vec{x} \). Thus, effective predicate abstraction — and program analysis tasks in general — requires a mechanism that combines space-efficient representation of formulas and fast QELIM.

This is challenging because QELIM algorithms require a formula in Disjunctive Normal Form (DNF), but DNF is a space-inefficient representation, e.g., relative to Conjunctive Normal Form (CNF). Common solutions to this issue follow one of three approaches: DNF, Abstract Syntax Tree (AST), and Decision Diagram (DD). In the DNF approach, a formula is represented by the set of terms of a DNF, e.g., a disjunctive invariant is represented by a set of octagons [15]. This approach is easy to implement, but does not scale to formulas with large DNFs. In the AST approach, a formula is represented as an AST (or a DAG) whose nodes correspond to variables, constants, and operators. This is the most space-efficient representation. However, converting an AST into DNF during QELIM — e.g., using a SMT-solver [12] — is expensive, in many cases exponential in the AST size. In the DD approach, a formula is represented by a DAG whose nodes are labeled by atomic terms. The DAG enables sharing of sub-expressions, and, at the same time, is easy to convert to DNF. This is the approach we explore in this paper by introducing and evaluating a new data structure, Linear Decision Diagram (LDD), for quantifier-free first-order linear arithmetic (LA) formulas.

LDDs extend DDDs — decision diagrams for difference logic — proposed by Møller et al. [16]. Predicates in difference logic are of the form \( x - y \leq c \) or \( x - y < c \) for variables \( x, y \) and a constant \( c \), ranging over \( \mathbb{Q} \) or \( \mathbb{Z} \). The key idea of DDDs is to represent first-order quantifier-free difference logic formulas as BDDs with nodes labeled by atomic predicates, and to reduce redundancy by leveraging implications between those predicates. For example, in a DDD, a node labeled with \( x - y \leq 10 \) never appears as a high child of a node labeled with \( x - y \leq 5 \). For a fixed variable order, a DDD of a formula \( f \) is no larger than a BDD representing a propositional abstraction of \( f \) (i.e., \( f \) with all atomic terms replaced by propositional variables). An important feature of DDDs is a QELIM algorithm based on Fourier-Motzkin elimination [3]. The algorithm lends itself well to dynamic programming, thus, leveraging the DAG-structure of DDs.

DDDs have three main limitations as an instrument to aid program analysis: (a) difference logic is too restrictive for many program analysis tasks, (b) DDDs do not support dynamic variable ordering (DVO), and (c) there are no publicly available implementations of DDDs and no reports of their effectiveness in solving practical program analysis problems. Our solution via LDDs address all three limitations. Specifically, LDDs extend to full linear arithmetic, and support efficient algorithms for DVO and QELIM. Moreover, we implemented LDD within CUDD, a state-of-the-art BDD package. Finally, we have evaluated LDDs using a benchmark derived from open-source programs.

Extending the Boolean operations from DDDs to LDDs is straightforward. The key challenges are in supporting DVO and QELIM. The importance of DVO for DDs is well-known. This is especially true for LDDs since they add restrictions on the variable order. We show that the standard BDD DVO cannot be used as is for LDDs. Instead, we adapt Rudell’s sifting algorithm [18], as implemented in CUDD. Our adaptation does not add any overhead over the BDD version of DVO. Our experiments confirm that DVO reduces the size of LDDs significantly.
We develop two types of QELIM for LDDs. The black-box QELIM applies an external QELIM-solver to each path in the LDD. It is linear in the number of paths (bad), but is compatible with any off-the-shelf solver (good). In contrast, the white-box QELIM is a generalized and optimized variant of the DDD version. It recursively applies pairwise resolution to DD nodes, in the style of Fourier-Motzkin. In the worst case, this algorithm is exponential in the size of the diagram. However, our experiments indicate that it performs well in practice. Black-box and white-box QELIM have success rates of 4.47% and 98.94%, respectively, when solving our benchmark problems.

The basic white-box QELIM algorithm only eliminates one variable at a time—a fundamental limitation of Fourier-Motzkin. However, many applications of QELIM in program analysis require eliminating multiple variables. To address this, we present an elimination strategy that iterates, while there are variables to be eliminated, between (a) dropping constraints with variables that are not resolved on during Fourier-Motzkin, and (b) choosing and eliminating an existentially quantified variable which results in a minimum number of resolutions. This heuristic yields a speedup of over 5 times for QELIM in our benchmark.

In order to test the suitability of LDDs for solving practical program analysis programs, we have evaluated our implementation on a benchmark derived from open source programs. The benchmark consists of transition relations (in Static Single Assignment form) of 850 functions from 25 C programs. In each case, we measured the space required (in DD nodes) to represent the transition relation, and time to compute a forward image (i.e., strongest post-condition). The experimental results lead us to believe that LDDs are an effective representation for fragments of LA for program analysis tasks.

Related Work. DDs for theories other than propositional logic have been studied extensively since the early 90’s, capitalizing on the great success of BDDs and numerous BDD optimizations. Among these, we do not cover DDs—such as Binary Moment Diagrams (BMDs) [5], Algebraic Decision Diagrams (ADDs) [2], and Boolean Expression Diagrams (BEDs) [1]—which are restricted to variables with finite domains. Thus, the most relevant structures to LDDs are those that label the nodes with linear predicates over the reals.

Groote and Tveretina [9] proposed decision diagrams for full first-order logic. Assuming an input formula is in Prenex normal form, they represent the negation of its quantification suffix with a DD, and prove a contradiction using Skolemization and standard strategies, e.g., applying unifiers.

Equational (EQ) BDDs [10] are aimed at deciding equalities with uninterpreted functions (EUF). In EQ-BDDs, nodes are labeled with predicates (equalities), and reduction rules enforce substitution according to a predefined order ≤ between variables. For example, if \( x \leq y \), then \( y \) is substituted by \( x \) in high sub-DD of a node labeled \( x = y \). Equational BDDs are semi-canonical—they reduce to \( 0 \) (or \( 1 \)) if they represent a contradiction (or tautology), but are non-canonical otherwise.

Cavada et al. [6] propose a QELIM technique for LA that combines BDDs and SMT-solvers. They focus on predicate abstraction, and consider the problem of quantifying all numeric variables from LA formulas (see (1) for a template) over LA predicates and propositional variables. The Boolean structure of the formulas are encoded via BDDs. QELIM is done by recursively traversing the BDD, carrying, along each path, the set of linear predicates (i.e., the context) seen on it. At each recursive step, an SMT-solver is used to check whether the context is consistent. Paths with inconsistent context are removed. The use of the context precludes the use of dynamic programming. Thus, the algorithm is linear in the number of paths of the BDD. We call such an approach “black box” because it uses an external decision procedure as is. In Sec. IV, we present a similar “black box” algorithm for quantifying some or all numeric variables.

The most relevant prior work is on DDDs [16]. QELIM of a numeric variable from a DDD is based on Fourier-Motzkin. Although in the worst case this procedure is exponential in the size of the DD, in the best case it is the same as QELIM for BDDs. We describe it in more detail in Sec. IV, as it is the base for our improved method. Clock Difference Diagrams [13], is an alternative to DDDs that was developed independently around the same time. CDDs are based on DDDs with arbitrary branching degree. QELIM is done in the black-box fashion by traversing all I-paths. We are not aware of any work that has adapted DVO to either DDDs, CDDs, or EQ-BDDs. DDDs and CDDs are extensions of Interval Decision Diagrams (IDD) [19].

We define LDDs in the next section. In Sec. III and IV we discuss the problems of dynamic variable ordering and QELIM with such diagrams, respectively. Sec. V is dedicated to experimental results, and we conclude in Sec. VI.
$T$ defined as follows: $exp(0)$ is $\text{FALSE}$, $exp(1)$ is $\text{TRUE}$, otherwise, $exp(u)$ is defined recursively as:

$$exp(u) = \text{ITE}(C(u), exp(H(u)), exp(L(u))) ,$$

where

$$\text{ITE}(a, b, c) = (a \land b) \lor (\neg a \land c) .$$

For simplicity, we don’t distinguish between a node $u$ and $exp(u)$.

**Example 1** An example of an LDD for the formula

$$(z - y \leq 0 \land x - y \leq 10) \lor (z - y > 0 \land x - y \leq 5)$$

is shown in Fig. 3(a). A different LDD for the same formula, owing to a different order, is shown in Fig. 3(b).

**B. Requirements from the theory**

A theory $T$ over variables $Var$ is LDD-adequate, or simply adequate, if for any given set of consistent $T$-atoms $A_T$ over $Var$ (e.g., $x < x$ is an inconsistent $T$-atom for $T$ being linear arithmetic), the following functions can be provided:

- **(Negation)** $\text{NEG} : A_T \mapsto A_T$ such that $\text{NEG}(c) \iff \neg c$.

In the following, we write $\neg c$ to mean $\text{NEG}(c)$.

- **(Normalization)** $\text{N} : A_T \mapsto A_T$ such that if $c \equiv c'$ or $c \equiv \neg c'$ then $N(c) = N(c')$. Note that if $c \in A_T$, $N(c) = N(\neg c)$. If $c = N(c)$, then $c$ and $\neg c$ are represented by $\text{ITE}(c, 1, 0)$ and $\text{ITE}(c, 0, 1)$, respectively.

- **(Negation Check)** $\text{isNEG} : A_T \mapsto \text{Bool}$ such that $\text{isNEG}(c) \iff \neg \text{NEG}(c)$.

- **(Implication)** $\text{IMP} : A_T \times A_T \mapsto \text{Bool}$ such that $\text{IMP}(c_1, c_2) \iff (c_1 \Rightarrow c_2)$.

- **(Resolution)** $\text{RSLV} : A_T \times A_T \mapsto \text{A}_{T \cup \{ \text{true} \}}$ such that $\text{RSLV}(c_1, c_2) = c_3 \iff x \in \text{VAR}(c_1) \cap \text{VAR}(c_2)$, and $c_3 \iff \exists x \cdot c_1 \land c_2$. We syntactically extend $\text{RSLV}$ so its first argument is a set of $T$-atoms as follows:

$$\text{RSLV}(S, x, c) = \bigwedge_{s \in S} \text{RSLV}(s, x, c) .$$

**Example 2** Let UTVPI be the quantifier-free first order theory of Unit Two Variables Per Inequality over the integers. The set of UTVPI-atoms is

$$\{ax + by \leq k \mid x, y \in Var, a, b \in \{-1, 1\}, k \in \mathbb{Z} \} .$$

This theory is also known as Octagons [15]. UTVPI is adequate, as shown below:

- $\text{NEG}(ax + by \leq k) = \neg ax - by \leq -k - 1$.

- Let $< v$ be a total order on $Var$ and $c = ax + by \leq k$. Then, $N(c)$ is (i) $N(by + ax \leq k)$ if $y <_v x$, (ii) $c$ if $x <_v y \land a > 0$, and (iii) $\text{NEG}(c)$ otherwise.

- $\text{IMP}(c_1, c_2) = \text{TRUE}$ iff $c_1 = ax + by \leq k$ and $c_2 = ax + by \leq k'$ and $k \leq k'$.

- $\text{RSLV}(c_1, x, c_2)$ is true if $x$ does not appear in opposite phases in $c_1$ and $c_2$. Otherwise, it is the result of resolution on $x$ between $c_1$ and $c_2$. For example, $\text{RSLV}(x - y \leq 5, x, z - x \leq 2) = z - y \leq 7$.

Other adequate theories include: intervals, whose atoms are $\{x \leq k \mid x \in Var, k \in \mathbb{Z} \}$; difference logic, whose atoms are $\{x \leq k \mid x \in Var, k \in \mathbb{Z} \}$. These theories are adequate in the sense that they obey the axioms of adequacy.

**1. function MK (A_T c, LDD f, LDD g)**

2. **if** (IMP(c, C(f))) **then** $f \leftarrow H(f)$

3. **if** ($f = g$) **then return** $g$

4. **if** (IMP(c, C(g)) $\land f = H(g))$ **then return** $g$

5. **return BDDNODE(c, f, g)**

Fig. 1. MK: Building an LDD.

\{x - y \leq k \mid x, y \in Var, k \in \mathbb{Z} \}; and linear arithmetic over the reals. We use UTVPI for illustrations in this paper and in all of our experiments.

**C. Variable ordering**

For LDDs, “$T$-atoms ordering” replaces the traditional BDD “variable ordering”. Ordering between the $T$-atoms facilitates the construction of reduced diagrams. Let $\leq_{\text{IMP}}$ be the partial order on $A_T$ induced by $\text{IMP}$: $c_1 \leq_{\text{IMP}} c_2 \Leftrightarrow \text{IMP}(c_1, c_2)$. A $T$-atoms ordering is any total order $\leq_T$ that extends $\leq_{\text{IMP}}$ to a total order on $A_T$. An LDD $u$ is ordered w.r.t. $\leq_T$ iff for every node $v$ reachable from $u$, $C(v) \leq_T C(H(v))$ and $C(v) \leq_T C(L(v))$. An LDD $u$ is well-ordered if it is ordered with respect to some $T$-atoms ordering $\leq_T$. Both of the LDDs in Fig. 3 are well-ordered.

**D. Local Reductions**

An LDD is locally reduced iff the following five conditions hold on every internal node $u$ and $v$.

1. No duplicate nodes. $\text{attr}(u) = \text{attr}(v) \Rightarrow u = v$.

2. No redundant nodes. $L(v) \neq H(v)$.


4. Imply high. $\neg \text{IMP}(C(v), C(L(v)))$.

5. Imply low. $\text{IMP}(C(v), C(L(v))) \Rightarrow H(v) \neq H(L(v))$.

For example, the LDD in Fig. 3(a) is reduced, but the LDD in Fig. 3(b) is not. From here on, we write LDD to mean Reduced Ordered LDD (ROLDD). The function MK($c$, $f$, $g$), shown in Fig. 1, constructs an ROLDD for $\text{ITE}(c, f, g)$, where (i) $c$ is a normalized constraint, (ii) $f$ and $g$ are ROLDDs s.t. $f \neq g$, and (iii) $c \leq_T C(f)$ and $c \leq_T C(g)$. Lines 2–4 ensure that the result is reduced, and line 5 returns a unique diagram node representing the $\text{ITE}$. The proof of correctness of MK is based on the following two reduction rules to enforce $\text{Imply high}$ and $\text{Imply low}$, respectively:

\[
\begin{align*}
\text{ITE}(x, \text{ITE}(y, h, l), z) & \quad \text{IMP}(x, y) \\
\text{ITE}(x, h, z) & \\
\text{ITE}(x, y, \text{ITE}(z, h, l)) & \quad \text{IMP}(x, z) \quad y \leftrightarrow h \\
\text{ITE}(z, h, l) &
\end{align*}
\]

**E. Basic LDD Operations**

For any symmetric operator $op$ that distributes over $\text{ITE}$, the function $\text{APPLY}$ (Op $op$, LDD $f$, LDD $g$) constructs the LDD for $f$ $op$ $g$. It is similar to the equivalent BDD operation. It is based on the following transformations (if multiple rules apply, the earliest is selected) and their symmetric versions obtained by swapping the arguments of $op$:

\[
\text{ITE}(x, y, z) \quad op \quad \text{ITE}(u, v, w) \quad x \leftrightarrow u \\
\text{ITE}(x, y \quad op \quad z \quad op \quad w) 
\]
function SWAPINPLACE(i, j)
replace every BDD node F : (i, H, L) with (j, G₁, G₀)
where
F₁₀, F₁₁ are the ¬j and j cofactors of H
F₀₀, F₀₁ are the ¬j and j cofactors of L
G₁ ← (F₁₁ = F₀₁) ? F₁₁ : (i, F₁₁, F₀₁)
G₀ ← (F₀₀ = F₁₀) ? F₁₀ : (i, F₁₀, F₀₀)

Fig. 2. Swapping adjacent labels in a BDD.

\[
\text{ITE}(x, y, z) \oplus \text{ITE}(u, v, w) \quad \text{IMP}(x, u), \quad \text{ITE}(x, y \oplus v, z \oplus \text{ITE}(u, v, w)) \quad x \leq T
\]

LDD conjunction (AND) and LDD disjunction (OR) are implemented via APPLY. LDD negation (NOT) is implemented as in BDDs. The implementation of ternary LDD if-then-else (ITE) is similar to APPLY.

In summary, extending Boolean operations from BDDs to LDDs is straightforward. In the next two sections, we show how to extend dynamic variable ordering and QELIM, which are more challenging.

III. Dynamic Variable Ordering

It is well known that the variable order of a decision diagram has a crucial effect on its size. Both finding the best order and deciding whether an order is optimal are NP-hard [4]. A lot of BDD research (e.g., [18], [8], [17]) has been dedicated to heuristics for finding a good variable order. In this section, we show how to adapt the sifting heuristic of Rudell [18], as implemented in CUDD, to LDDs. The exact details of the heuristic are beyond the scope of this paper. We only focus on the parts that we changed.

Sifting heuristic is based on trial-and-error. Each node label (i.e., a BDD variable) is moved up and down in the order by swapping the order of two adjacent labels. The best position is recorded and restored at the end. There are several factors that make sifting very efficient: a set of Boolean functions is represented as one multi-rooted DAG; a unique table is used to locate nodes in the DAG in constant time; the table is partitioned into subtables, one per label, to locate all nodes with a given label in O(1); and, finally, swapping adjacent labels i and j in all diagrams in the unique table is done in time linear in the number of nodes labeled with i or j.

Only the swapping algorithm needs to be adapted for LDDs. Swapping adjacent labels amounts to reordering diagrams in the unique table. In CUDD, this operation is called SWAPINPLACE. We first show how SWAPINPLACE works for BDDs, and then, that it does not work for LDDs.

Pseudocode for SWAPINPLACE is shown in Fig. 2. Note that the swapping is done in place — any edge that was pointing to a node labeled with i before the swap points to the same node, but now labeled with j after the swap. Furthermore, SWAPINPLACE maintains an invariant that every diagram in the unique table is well-ordered and reduced.

SWAPINPLACE does not work for LDDs. Consider an LDD shown in Fig. 3(a). Completely unrestricted swapping of adjacent labels conflicts with LDD well-orderness constraints.

1: function LDDSWAPINPLACE(A₁, x, A₂, y)
2: replace every LDD F : (x, H, L) with (y, G₁, G₀), where
3: F₀₀, F₀₁ are the ¬y and y cofactors of L
4: F₁₀, F₁₁ are the ¬y and y cofactors of H
5: F₁₁ ← IMP(y, C(F₁₁)) ? H(F₁₁) : F₁₁
6: F₀₁ ← IMP(y, C(F₀₁)) ? H(F₀₁) : F₀₁
7: if (F₁₁ = F₀₁) \lor (IMP(x, C(F₀₁)) \land F₁₁ = H(F₀₁)) then
8: G₁ = F₀₁
9: else G₁ ← (x, F₁₁, F₀₁)
10: if (F₀₀ \lor (IMP(x, C(F₀₀)) \land F₀₀ = H(F₀₀)) then
11: G₀ = F₀₀
12: else G₀ ← (x, F₁₀, F₀₀)

Fig. 5. Swapping adjacent labels in an LDD.
function bbQE (LDD \( f, P \subseteq T\)-atoms, \( V \subseteq Var \))
1. if \((f = 1)\) then return \( \text{TO} \)D\( (\text{thQELIM}(V, P)) \)
2. if \((f = 0 \lor \text{UNSAT}(P)) \) then return 0
3. \( c \leftarrow C(f) \)
4. \( \text{if} (V \cap \text{VARS}(c) \neq \emptyset) \) then
5. \( t \leftarrow \text{bbQE}(H(f), P \cup \{c\}, V) \)
6. \( e \leftarrow \text{bbQE}(L(f), P \cup \{-c\}, V) \)
7. \( \text{return OR}(t, e) \)
8. else
9. \( t \leftarrow \text{bbQE}(H(f), P, V) \)
10. \( e \leftarrow \text{bbQE}(L(f), P, V) \)
11. \( \text{return ITE}(c, t, e) \)

Fig. 6. Black-box QELIM.

Correctness of GROUPMOVE. Let \( G = (V, E) \) be a multi-rooted DAG of LDDs. A set of \( T\)-atoms \( X \) is closed for \( G \) iff whenever \( x \in X \) and there is a \( v \in V \) s.t. \( \text{IMP}(C(v), x) \) or \( \text{IMP}(x, C(v)) \), then \( C(v) \in X \). The correctness follows from Theorem 1.

**Theorem 1** Let \( G = (V, E) \) be a multi-rooted DAG of RO-LDDs, and \( X, Y \) be two non-empty sets of \( T\)-atoms that are closed and adjacent in \( G \). Let \( G' = (V', E') \) be the DAG after GROUPMOVE\((X, Y)\). Then, (i) \( G' \) is a DAG of RO-LDDs, and (ii) for any node \( v \) in \( G \) and the same node \( v' \) in \( G' \), \( \exp(v) = \exp(v') \).

IV. EXISTENTIAL QUANTIFICATION FOR LDDs

In this section, we describe three techniques for QELIM over LDDs. In the algorithms, TO\( \)D\( D \) is used to convert a set \( P \) of \( T\)-atoms into an LDD for \( \bigvee P \); ITE and OR mean the corresponding LDD operations. For simplicity, we do not distinguish between a single \( T\)-atom and the corresponding LDD.

A. Black-box QELIM

Our black-box QELIM (see Fig.6) is called bbQE. It applies an external theory QELIM to each path of an LDD. bbQE requires the following helper functions from the theory:

- \( \text{UNSAT}(P) \) decides whether \( \bigwedge P \) is unsatisfiable;
- \( \text{QELIM}(V, P) \) given a set of variables \( V \) and a set of \( T\)-atoms \( P \), computes a set of \( T\)-atoms \( P' \) s.t. \( \bigwedge P' \) is equivalent to \( \exists V \cdot \bigwedge P \).

Running time of bbQE\((f, P, V)\) is linear in the number of paths of \( f \). bbQE is not compatible with dynamic programming since it propagates the context \( P \) along every branch of an LDD.

B. White-box QELIM

Our white-box QELIM applies Fourier-Motzkin (FM) elimination directly to LDDs. It extends the QELIM algorithm of DDDs [16] to any adequate fragment of T-LA.

First, we briefly recall FM elimination [3]. Let \( \varphi \) be a conjunction of \( T\)-atoms, and \( x \) be a numeric variable. FM elimination of \( x \) from \( \varphi \) proceeds as follows: Initially \( S \) is the set of all atoms of \( \varphi \), and \( S' = \emptyset \). For each \( p \in S \), remove \( p \) from \( S \). If \( x \notin \text{VARS}(p) \) then add \( p \) to \( S' \); otherwise, for each \( t \in S \) s.t. \( x \in \text{VARS}(t) \) add \( \text{RSLV}(p, x, t) \) to \( S' \). Note that \( \text{RSLV}(p, x, t) \) is defined to be \( \text{TRUE} \) when \( x \) occurs in the same phase in both \( p \) and \( t \). Upon termination, \( \bigwedge S' \) is equivalent to \( \exists x \cdot \varphi \).

The key insight of white-box QELIM is that FF simultaneously to every 1-path of an LDD. The main step is simultaneous resolution. It is done by a function DR\((S, x, f)\) (short for DAGRESOLVE) that takes a set \( S \) of \( T\)-atoms, a variable \( x \), and an LDD \( f \), and returns an LDD obtained by adding to each 1-path \( \pi \) of \( f \) the resolvents of \( S \) and \( \pi \) on \( x \).

DR is implemented as follows: if \( f \) is a constant, it returns \( f \); otherwise, it applies one of the recurrences shown in Fig. 7.

When implemented with dynamic programming, the number of recursive calls to DR is linear in the number of nodes in \( f \). However, at the end it needs to restore orderedness, which, like in DDDs, is exponential in the size of \( f \) in the worst case.

The basic white-box algorithm wbQE1\((x, f)\) is shown in Fig. 8. At each iteration, the algorithm either descends to branches of \( f \) (line 4), or removes a top-node of \( f \) whose label contains \( x \) (lines 5–7). The algorithm terminates since at each iteration the number of nodes labeled with an atom containing \( x \) decreases.

Recall that variable ordering in LDDs always respects chains of implications among \( T\)-atoms. Consider a “low implication chain” of LDD nodes \( u_1, \ldots, u_n \). That is,

\[
\forall 1 \leq i < n \cdot L(u_i) = u_{i+1} \land C(u_i) \Rightarrow C(u_{i+1}.
\]

Then, \( \forall 1 \leq i < n \cdot \neg C(u_n) \Rightarrow \neg C(u_i) \). Let \( c \) be a \( T\)-atom and \( x \in Var \). Then,

\[
\forall 1 \leq i < n \cdot \text{RSLV}(\neg C(u_n), x, c) \Rightarrow \text{RSLV}(\neg C(u_i), x, c).
\]

Let \( S \) be a set of \( T\)-atoms. Then,

\[
\text{RSLV}(\neg C(u_1), \ldots, \neg C(u_n)) \cup S, x, c \Leftrightarrow \text{RSLV}(\neg C(u_n)) \cup S, x, c
\]

We use this observation in the algorithm wbQE2 (see Fig. 9) to reduce the number of calls to DR.

Since wbQE2\((x, f)\) uses DR, in the worst case it is exponential in the number of nodes in \( f \). However, in the best case it has the same complexity as BDD QELIM.

C. Eliminating Multiple Variables

Unlike bbQE, white-box QELIM only eliminates one variable at a time – this is a fundamental limitation of Fourier-Motzkin. When eliminating multiple variables, the order in which they are eliminated is crucial. For example, consider a formula

\[
x - y \leq 1 \land z - x \leq 2 \land w - z \leq 3.
\]
Assume we want to eliminate \( x \) and \( y \). There are two elimination orders: (a) \( x \), \( y \), and (b) \( y \), \( x \). In case (a), first \( x - y \leq 1 \) is removed and resolved with \( z - x \leq 2 \) to get: \( z - y \leq 3 \wedge z - x \leq 2 \wedge w - z \leq 3 \). Then, \( z - x \leq 2 \) is dropped, and finally \( z - y \leq 3 \) is dropped to get: \( w - z \leq 3 \). In case (b), first \( x - y \leq 1 \), and then \( z - x \leq 2 \) are dropped. No resolution is needed.

This example highlights two things. First, eliminating variables that occur in fewer atoms (like \( y \) above) leads to fewer resolutions and potentially smaller intermediate results. Second, variables that occur in a single atom (like \( y \) above), or, more generally, variables that occur in pure polarity in a disjunct of a DNF, are eliminated by dropping their atoms without any resolution steps. Since there is no resolution, multiple such variables can be eliminated at once.

We use these observations in a multi-variable elimination strategy called \( \text{wbMVQE} \) shown in Fig. 10. \( \text{wbMVQE} \) is parametrized by two functions:

- \( \text{FINDDROPVARS}(V, f) \) returns the subset of variables in \( V \) that do not need to be resolved on when they are eliminated from an LDD \( f \).
- \( \text{CHOOSEVAR}(V, f) \) chooses a variable in \( V \) to be eliminated from an LDD \( f \).

It also uses a helper function \( \text{dRVAR}(V \subseteq \text{Var}, \text{LDD } f) \) shown in Fig. 11 that disjunctively drops all nodes from an LDD \( f \) that are labeled with an atom containing a variable in \( V \).

\( \text{wbMVQE} \) iterates through two phases. First, it eliminates all variables that do not need resolution (lines 4–8). This is repeated until no more variables can be dropped. Second, it eliminates a variable using \( \text{wbQE2} \) (lines 9–10). This process repeats until all variables are eliminated.

Note that \( \text{wbMVQE} \) is only a strategy—it must be instantiated with an implementation of \( \text{FINDDROPVARS} \) and \( \text{CHOOSEVAR} \). For our experiments, we have instantiated \( \text{wbMVQE} \) by counting the number of occurrences of variables in \( V \) in the atoms labeling the nodes of \( f \) (i.e., the support of \( f \)). In our case, \( \text{FINDDROPVARS} \) returns all variables that occur in only a single atom; \( \text{CHOOSEVAR} \) picks a variable randomly from all variables that occur in the least number of atoms.

**V. Experimental Results**

We have implemented LDDs within CUDD. Except for DVO, our implementation is an external library that adds, but does not modify, CUDD. Following CUDD, we use complemented edges which allow for constant time negation. For DVO, we reuse all CUDD’s heuristics, but modify how adjacent labels are swapped (see Sec. III). Fortunately, CUDD already can group variables and sift groups simultaneously (i.e., \( \text{GROUPMOVE} \)), but we had to change its implementation of \( \text{GROUPMOVE} \) to sift top-down instead of bottom-up.

To evaluate our implementation, we used a benchmark derived from 25 real C programs, including \text{mplayer}, \text{ffmpeg}, \text{gzip}, \text{tcsh}, and CUDD. We created the benchmark by compiling each program using LLVM [14] with optimization, loop unrolling, and inlining enabled, and then approximating the SSA control-flow graph of each function by a UTVPI formula. In general, our approximation is unsound since we replaced LA formulas by UTVPI. However, each such formula is similar in structure to a bounded model-checking problem, e.g., as in CBMC [7]. We narrowed down the initial 10,000 formulas to our benchmark of 850 using the criteria: (a) more than 1,000 nodes in LDD or BDD representation, or (b) more than 2 seconds to build an LDD or a BDD, or (c) more than 2 seconds to solve with SVO.
These formulas range in sizes from 4KB to 700KB, and have between 30 to 7,956 variables.

We conducted two sets of experiments to evaluate the effect of local LDD reductions and the effectiveness of QELIM, respectively. All experiments were done on an 8-core 2.00GHz Xeon with 3GB of RAM. Each test-case was limited to 300s of CPU and 512MB of RAM. The benchmark and detailed experimental results are available at www.sei.cmu.edu/staff/chaki/FMCAD-09.html.

**Local Reductions.** To measure the effect of local reductions, we compared the sizes of LDD vs. BDD for each test-case using both SVO and DVO. By “BDD” we mean a BDD constructed by abstracting all UTVPI predicates by propositional variables. For BDDs, SVO is a syntactic variable order where each new predicate is placed at the end of the current order. It is the same for LDDs, except when it violates the LDD ordering restriction: in that case, the new predicate is inserted at an appropriate position in the order. For example, for the formula $x - y \leq 5 \land y - z \leq 0 \land x - y \leq 15$, the BDD SVO is as seen in the formula, while the LDD SVO is $x - y \leq 5, x - y \leq 15, y - z \leq 0$. DVO means that automatic DVO was enabled and DD manager reordered whenever memory usage was high.

The results are summarized in the scatter plot in Fig. 12. It shows LDD sizes (x-axis) vs. BDD sizes (y-axis). For example, the point $(325, 720)$ means that some test-case had an LDD with 325 nodes and a BDD with 720 nodes. Both axes are in log-scale. SVO and DVO experiments are marked by diamonds and crosses, respectively. As expected, DVO leads to significantly smaller diagrams for both BDDs and LDDs. Interestingly, with DVO LDDs are significantly smaller (sometimes by an order of magnitude) than BDDs, whereas with SVO the situation is reversed. This validates our intuition that DVO is even more significant for LDDs than for BDDs.

**Quantification.** To evaluate the effectiveness of our QELIM algorithms, we measured the time to quantify out the first 4/5\textsuperscript{th} syntactically appearing variables in each test-case. This roughly corresponds to a forward-image (a.k.a. strongest post-condition) in program analysis. We compared BB\textsc{Q}E and 4 variants of WB\textsc{MVQE} (DVO is used unless stated otherwise):

- \textsc{wb+SVO}: with SVO,
- \textsc{wb+DVO}: with DVO,
- \textsc{wb-DV}: with lines 4–8 removed, and
- \textsc{wbWB1}: with a call to wb\textsc{QE2} on line 10 replaced with the call to wb\textsc{QE1}.

The overall results are summarized in Table I. We call the 696 test-cases that are solved by \textsc{wb+SVO} in under 15s \textsc{easy}, and the remaining 154 \textsc{hard}. Total is the time including parsing, building an LDD, and QELIM; \textsc{QE} is the time spent in BB\textsc{Q}E or WB\textsc{MVQE}. All times are in seconds. Each failure is normalized to 300s. Size of the final LDDs ranged from 140, 092 to 1.

**TABLE I**

<table>
<thead>
<tr>
<th>Alg.</th>
<th>Total \textsc{QE}</th>
<th>\textsc{TO}</th>
<th>\textsc{MO}</th>
<th>Total \textsc{QE}</th>
<th>\textsc{TO}</th>
</tr>
</thead>
<tbody>
<tr>
<td>BB\textsc{Q}E</td>
<td>—</td>
<td>—</td>
<td>141</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>WB\textsc{DVO}</td>
<td>10,953</td>
<td>3,329</td>
<td>9</td>
<td>0</td>
<td>784</td>
</tr>
<tr>
<td>WB\textsc{SVO}</td>
<td>38,739</td>
<td>36,511</td>
<td>21</td>
<td>99</td>
<td>395</td>
</tr>
<tr>
<td>WB\textsc{WB1}</td>
<td>11,047</td>
<td>3,761</td>
<td>11</td>
<td>0</td>
<td>829</td>
</tr>
<tr>
<td>WB\textsc{DV}</td>
<td>17,043</td>
<td>13,358</td>
<td>34</td>
<td>0</td>
<td>5,649</td>
</tr>
</tbody>
</table>

**Fig. 12.** Size comparison in DD nodes between LDD and BDD.

**Fig. 13.** Total times for white-box QELIM.
In this paper, we have tackled the problem of space-efficient representation of LA formulas with support for Boolean operations and QELIM. This problem is at the heart of many program analysis tasks. To this end, we have extended Difference Decision Diagrams to Linear Arithmetic. Our key contributions are: support for Dynamic Variable Ordering, QELIM algorithms, an implementation inside CUDD, and empirical evaluation on a large benchmark derived from real programs.

Overall, we found that LDDs in combination with DVO and dynamic programming-based QELIM algorithm leads to an effective data structure for program analysis tasks.

We believe that LDDs is a good basis for a combined predicate and numeric abstract domain, in the style of [11]. We plan to explore this direction in future work.

VI. CONCLUSION

In this paper, we have tackled the problem of space-efficient representation of LA formulas with support for Boolean operations and QELIM. This problem is at the heart of many program analysis tasks. To this end, we have extended Difference Decision Diagrams to Linear Arithmetic. Our key contributions are: support for Dynamic Variable Ordering, QELIM algorithms, an implementation inside CUDD, and empirical evaluation on a large benchmark derived from real programs.

Overall, we found that LDDs in combination with DVO and dynamic programming-based QELIM algorithm leads to an effective data structure for program analysis tasks.

We believe that LDDs is a good basis for a combined predicate and numeric abstract domain, in the style of [11]. We plan to explore this direction in future work.

REFERENCES