Two Theorems on Improving the SUP-INF Method

by

Michael Lacey

December 1979 ATP-55

Two Theorems on Improving the SUP-INF Method

Abstract. The SUP-INF technique tests for consistency of a set T of ground inequality literals, by computing and comparing the number SUP x and INF x, for each term x appearing in T. A theorem is proved which shows that when new entries are made to T, the computation of SUP x and INF x need only be made for x's appearing in the added entries. A similar theorem is proved about finding equalities implied by T.

In his paper "The SUP-INF Method in Presburger Arithmetic," Bledsoe introduced the algorithms SUP and INF designed to calculate the maximum and minimum, respectively, of a variable subject to a set of linear constraints. Both [1,2] and Shostak [3] have devised methods, utilizing these two algorithms, to determine the validity, as well as the invalidity, of a class of formulas that arise in Program Verification - Presburger formulas with universally quantified variables. This article presents two theorems which improve the efficiency of part of the method described in [2]. The theorems apply to the case when new entries are made to a satisfiable set of linear inequalities, to form an augmented set T. The validity of T can be established by calculating and comparing SUP x and INF x only for those variables occurring in the added entries.

In the next sections the original procedure is described, and the improvements. Following that, the theorems are presented and proved.

2. The Original Method

Given a conjunction of universally quantified linear inequalities, $L_1 \le M_1 \wedge, \ldots \wedge L_i \le M_i$, and V, the set of variables that occur in the inequalities, we first rewrite the inequalities as S, a set of inequalities of the form

$$\mathrm{LOWER}_S(x) \leq x \leq \mathrm{UPPER}_S(x)$$

for all $x \in V$. $\mathrm{UPPER}_S(x)$ is obtained by solving all the inequalities $L_j \leq M_j$ in terms of x; consider the inequalities $\{x \leq U_1, \ldots, x \leq U_r\}$. $\mathrm{UPPER}_S(x)$ is then

$$\mathrm{UPPER}_S(x) = \begin{cases} \mathrm{MIN}(U_1, \ldots, U_r) & \text{if } 1 \leq r \\ U_1 & \text{if } r = 1 \\ \infty & \text{if } r = 0 \end{cases}$$

$\mathrm{LOWER}_S(x)$ is defined similarily.

For example, the conjunction

$$Y < 5 \wedge x + 2y < -2 \wedge -1 < y$$

would be converted into the set

$$S = \{-\infty < x < -2 - 2y,$$
$$-1 < y < \mathrm{MIN}(5, -1 - \tfrac{x}{2})\}$$

The recursive agorithms SUP and INF calculate the maximum and minimum values, respectively, of variables subject to such sets of linear constraints. The algorithms are functions of the variable whose maximum and minimum value is to be computed; the set of inequalities; and a list of variables initially set to NIL. For instance, in the example above

$$\mathrm{INF}_S(x,\emptyset) = -\infty;\ \mathrm{SUP}_S(x,\emptyset) = 0,$$
$$\mathrm{INF}_S(y,\emptyset) = -1;\ \mathrm{SUP}_S(y,\emptyset) = 5.$$

Given a set S of inequalities in the desired form, we check for the invalidity of S in two steps. First, $\mathrm{SUP}_S(v,\emptyset)$ and $\mathrm{INF}_S(v,\emptyset)$ are calculated and compared for each v occurring in S. If the interval

$$(1) \qquad \mathrm{INF}_S(v,\emptyset),\ \mathrm{SUP}_S(v,\emptyset)$$

is empty, we conclude that S is invalid. If no empty interval is found, we proceed to the second step in the procedure.

At this point we check for equality occurring in S, by testing to see if either

$$\mathrm{INF}_S(v,\emptyset) = \mathrm{SUP}_S(v,\emptyset)$$

$$\text{or} \quad \mathrm{SUP}_S(\mathrm{UPPER}_S(v), \{v\}) = v \tag{2}$$

is the case for any v occurring in S. Any equality units found are returned in the form of a substitution σ, which is applied to S to form the set $S\sigma$. Again, as in the first step, $\mathrm{INF}_{S\sigma}(v,\emptyset)$ and $\mathrm{SUP}_{S\sigma}(v,\emptyset)$ are calculated and compared. If an empty interval is found, then S is invalid. If no contradiction is found, we return $S\sigma$.

3. The Improved Method

The new method improved the old method's efficiency in the following case: Suppose an inequality is added to satisfiable set of linear inequalities, to form an augmented set T of inequalities. Let G be the set of variables occurring in the added inequality. The first step in the procedure is now to calculate and compare $\mathrm{INF}_T(v,\emptyset)$ and $\mathrm{SUP}_T(v,\emptyset)$ only for those v in G. If no contradiction is found, we conclude that for all v occurring in T, the interval

$$\mathrm{INF}_T(v,\emptyset),\ \mathrm{SUP}_T(v,\emptyset)$$

is non-empty, and proceed to the second part of the method.

In checking for equality (in the improved method), we check only one $u \in G$. If for this one u equality is not detected, then T implies no equality units that S does not imply. If equality is detected, we proceed as the old method does, by finding equality units; substituting equality units into $T\sigma$, and checking each variable in $T\sigma$ for a contradiction.

4. Preliminary Definitions.

Let V represent the set of variables $(v_1, v_2, \ldots, v_n)$, for some positive integer n. The following definitions are taken from [3] .

Definition. A linear form in V is an expression of the form

$$r_1v_1 + \ldots + r_nv_n + c,$$

where r_i is a non-negative real and c is a real.

Definition. A minilinear form in V is either a linear form in V, an expression of the form $MIN(L_1, L_2, \ldots, L_m)$ where $m \geq 2$ and each L_i is linear in V or one of ∞ or $-\infty$.

We assume all linear (minilinear) forms to be linear (minilinear) in V.

Definition. An inequality is an expression of the form $A \leq B$, where A and B are linear forms having no variables in common.

Definition. A point (with respect to V) is an assignment of reals to the members of V. If P is a point and Q is a minilinear form, the value of Q at P, written $Q(P)$, is the real obtained by evaluating Q in the customary way with each variable by its assignment in P.

Definition. If r is a real, Q is minilinear, and S is a set of inequalities, we say that Q can have the value r in S if there exists a point P satisfying S such that $Q(P) = r$. We say that Q has the unique value r in S if Q can have the value r in S, but no other value.

5. First Major Theorem

Let S be a satisfiable set of ground inequalitites in V of the form

$$\bigwedge_{i=1}^{n} (A_i \leq v_i \leq B_i)$$

with A_i and B_i minilinear.

Given an inequality of the form $A \leq B$ with A and B linear, let $G = (v_1, \ldots, v_k)$, for $k \leq n$, be the set of variables occurring in A and B. Further, suppose A and B have no variables in common. Intersect $A \leq B$ with S to form T. The first major theorem is then:

<u>Theorem 1</u>. If for some $v \in V$, the interval $INT_T(v,\emptyset)$, $SUP_T(v,\emptyset)$ is empty, then for some $u \in G$, $INT_T(u,\emptyset)$, $SUP_T(u,\emptyset)$ is empty.

Before the proof of this theorem can be given, we need the following lemma:

<u>Lemma 2</u> Let $\sigma: G \to$ Reals is a substitution; $L \subseteq V$; and A be minilinear. Then $SUP_{S\sigma}(A\sigma, L) = SUP_{T\sigma}(A\sigma, L)$.

Lemma 2 and its proof are similar to a theorem proved by Shostak [3] which appears in this paper as Theorem 8.

<u>Proof</u> All cases reduce to the one in which A is a single variable with $A \notin G$. That is $A\sigma = A$.

The proof is by recursive induction.

$SUP_{S\sigma}(A\sigma, L) = SUP_{S\sigma}(A, L)$

(2) $= SUPP(A, Z)$

where $Z = SUP_{S\sigma}(Q_{S\sigma}(A), L^{\cup}(A))$, and $Q_{S\sigma}(A) = UPPER_{S\sigma}(A)$

By induction hypothesis it follows that

(3) $Z = SUP_{T\sigma}(Q_{S\sigma}(A), L^{\cup}(A))$.

$A \notin G$, hence $Q_S(A) = Q_T(A)$, and

(4) $Q_{S\sigma}(A) = Q_{T\sigma}(A)$.

It follows from (3) and (4) that

(5) $Z = SUP_{T\sigma}(Q_{T\sigma}(A), L\ (A))$.

Substituting (5) into (2),

$$SUP_{S\sigma}(A,L) = SUPP(A,\ SUP_{T\sigma}(Q_{T\sigma}(A),\ L\ (A)))$$
$$= SUP_{T\sigma}(A,\ L)$$

As asserted, by the definition of SUP

The proof of Theorem 1 can now be given.

Proof of Theorem 1.

The proof is by contradiction. Assume that for all $u \varepsilon G$ the interval $[INF_T(u,\ \emptyset),\ SUP_T(u,\ \emptyset)]$ is not empty. We claim that for all $x \varepsilon V$, the interval $[INF_T(v,\ \emptyset),\ SUP_T(v,\ \emptyset)]$ is non-empty, in contradiction to the hypothesis.

To see this, first, for each $v_i \varepsilon G$ choose r_i so that

$$INF_T(vi,\ \emptyset) \leq r_i \leq SUP_T(vi,\ \emptyset).$$

And define σ:G→ Reals by $\sigma = (r_1/v_1,\ldots,r_k/v_k)$.

S is contained in T hence, it follows from Theorem 6 that

$$ri \leq SUP_T(v_i,\ \emptyset) \leq SUP_S(v_i,\ \emptyset)$$

Similarly

$$INF_S(v_i,\ \emptyset) \leq r_i.$$

Therefore, since S is satisfiable, $S\sigma$ is satisfiable. And so, for $v \varepsilon V-G$ the interval $INF_{S\sigma}(v,\ \emptyset),\ SUP_{S\sigma}(v,\ \emptyset)$, which by Lemma 2 is precisely the interval $INF_{T\sigma}(v,\ \emptyset),\ SUP_{T\sigma}(v,\ \emptyset)$, is non-empty. Therefore, for all $v \varepsilon V$, the interval $INF_T(v,\ \emptyset),\ SUP_T(v,\ \emptyset)$ is non-empty, which concludes the proof.

6. Preliminary Theorems

For these first few theorems we assume that S and T are satisfiable sets of linear inequalities. Also, the algorithms SUP and INF are mirror images of one another, so analogous statements hold for INF, but those statements are not explictly given. Lastly, when credit is not given, the theorem is due to Shostak.

Definition.
$$\mathrm{MAX}_S\ A = \begin{cases} r & \text{if } A \text{ can have the real value } r \text{ in } S, \text{ but no greater value.} \\ \text{undefined otherwise.} \end{cases}$$

Definition. S bounds R, a linear form, if for some real r, $\max_S R$ is defined and equal to r.

Definition. S minimally bounds R if S bounds R and no proper subset of S bounds R.

Theorem 3. Suppose S minimally bounds R. Then any point P that satisfies S such that $R(P) = \max_S R$ also satisfies S_E, a set of equalities obtained from S by replacing $\leq$ with $=$.

The following properties of SUP are needed for the proof of the second main theorem.

Theorem 4. (Bledsoe) If S is satisfiable, $\mathrm{SUP}_S(R,\emptyset) \leq \max_S R$.

Theorem 5. (Bledsoe) $\mathrm{SUP}_S(R,L)$ is a minilinear form in L.

Theorem 6. If T is contained in S, $\mathrm{SUP}_S(R,\emptyset) \leq \mathrm{SUP}_T(R,\emptyset)$.

<u>Theorem 7</u>. If A is a linear form with a unique value r in S, $SUP_S(A,\emptyset) = max_S A$.

<u>Theorem 8</u>. Say L, L' are sets of variables, L' contained in L, $\sigma:L-L' \to$ Reals a substitution, A is minilinear, and $SUP_S(A\sigma,L') \neq -\infty$. Then $SUP_{S\sigma}(A\sigma,L') = [SUP_S(A,L)]\sigma$.

<u>Definition</u>. T <u>implies equality</u> for $v \in V$ if either v has unique value in T, or $SUP_T(Q_T(v), \{v\}) = v$.

For the remainder of the paper, we assume that T is satisfiable, for simplicity's sake. This assumption will have no effect on it's application to the procedure described. Also, suppose that for some $u \in V$ T implies equality for u, but S does not. Denote by R a subset of T such that R implies equality for u, and no proper subset of R implies equality for v. We need to develop two properties of R. The first is as follows:

<u>Theorem 9</u>. A point P satisfies R if and only if P satisfies R_E.
<u>Proof</u>. Clearly, if P satisfies R_E, P satisfies R.

Suppose P satisfies R. If R minimally bounds u, then $u(P) = MAX_R U$, and so by theorem 3, P satisfies R_E. Consider the case when $SUP_R(Q_R(u), \{u\}) = u$. Let $\sigma:\{r/u\}$ be the substitution for u obtained from P. From Theorem 8

$$SUP_{R\sigma}(Q_R(u),\emptyset) = SUP_R(Q_R(u), \{u\})$$
$$= \{u\}\sigma = r.$$

Also, $INF_{R\sigma}(Q_R(u),\emptyset) = r$.

That is $R\sigma$ minimally bound $Q_R(u)$, hence P satisfies $R_{\sigma E}$, and therefore R_E.

This theorem is not yet in the form in which we need it. The following definition suggests an immediate corollary.

Definition. We write $A \equiv B$, where A and B are linear forms, if for all P that satisfy R, $A(P) = B(P)$.

Corollary 10. If $SUP_R(A,L) \neq \infty$, then $A \equiv SUP_R(A,L)$

Proof. All cases reduce to the one in which A is a single variable, $A \notin L$.

The proof is by recursive induction.

$SUP_R(A,L) = SUPP(A,Z)$ where $Z = SUP_R(Q_R(A), L \cup \{A\})$. And, by inspection of SUPP, $Z \neq \infty$.

Thus, by induction hypothesis, $Q_R(A) \equiv Z$. Furthermore, it follows from Theorem 9, that $A \equiv Q_R(A) \equiv Z$.

To complete the proof, we must inspect SUPP, to see that $SUPP(A,Z) \equiv A$. Assume Z is linear, that is Z is not of the form $MIN(B,C)$. $SUP_R(A,L) \neq \infty$, thus Z must be either linear in L, or of the form $bA + C$, where $b < 1$, and C is linear in L. In the latter case, we know $A \equiv bA + C$, which implies $A \equiv C/1\text{-}b$. And, by definition, $SUPP(A,Z) = C/1\text{-}b$. In the former case, $SUPP(A,Z) = Z$, which completes the proof.

7. Second Major Theorem.

Recall the assumptions made about T in the previous section; those assumptions are carried over into these last two theorems. The second major theorem is:

<u>Theorem 11</u>. Suppose T is satisfiable, and T implies equality for $v \in V$, whereas S does not imply equality for v. Then for all $u \in G$, T implies equality for u.

We actually show a slightly stronger result.

<u>Theorem 12</u>. For each u occurring in R, T implies equality for u.

To see that this theorem implies the former, note that R is not a subset of S, for otherwise, S would imply equality for v. Therefore, for some $g \in G$, either $UPPER_R(g)$ or $LOWER_R(G)$ is obtained from the inequality added to S to form T. Hence, all u in G occur in R.

<u>Proof</u>. Pick u occurring in R. Note that if u has unique value in R, the same condition holds in T. Similarly for the other condition of equality. Hence, it is sufficient to show that R implies equality for u.

Suppose, for r real, $SUP_R(u, \emptyset) = r$. Then by lemma 10, $u \equiv r$; that is, u has unique value in R.

Suppose $SUP_R(u,\emptyset) = \infty$. Pick r real, and let $\sigma:\{r/u\}$. Clearly, $INF_{R\sigma}(Q_R(u), \emptyset) = r$. And, as we saw earlier, $SUP_{R\sigma}Q_R(u), \emptyset) = r$. It follows from Theorem 8 that

$$[SUP_R(Q_R(u),\{u\})]\ \sigma = r.$$

we also know that

$$SUPR(u,SUP_R(Q_R(u),\{u\})) = \infty.$$

Therefore, $SUP_R(Q_R(u),\{u\}) = u$.

References

1. Bledsoe, W. W., "The SUP-INF Method in Presburger Arithmetic". Memo ATP-18, Department of Mathematics, University of Texas at Austin, Dec. 1979.

2. Bledsoe, W. W., Bruell, Peter, and Shostak, Robert. "A Prover for General Inequalities". Memo ATP-18, Department of Mathematics, University of Texas at Austin, Feb. 1979.

3. Shostak, Robert. "On the SUP-INF Method for Proving Presburger Formulas". JACM, Oct. 1977, pp. 529-543.

In a private communication, Robert Shostak reported a stronger result than theorem 1 of this article:

It T is a minimally contradicting set of inequalities, then for each variable v occurring in T, the interval $[\mathrm{INF}_T(V,\emptyset), \mathrm{SUP}_T(V,\emptyset)]$ is empty.