Symbolic Computation and Program Verification

Mădălina Eraşcu
Research Institute for Symbolic Computation
Johannes Kepler University, Linz, Austria
merascu@risc.uni-linz.ac.at

Abstract

We present methods for checking the partial correctness of, respectively to optimize, imperative programs, using polynomial algebra methods, namely resultant computation and quantifier elimination by cylindrical algebraic decomposition. The results are very promising but also show that there is room for improvement of algebraic algorithms.

1 Introduction

Using symbolic computation in program verification is a laudable goal, because the symbolic computation algorithms, although very powerful, have a high complexity which makes them difficult to solve program verification problems of significant size.

The mostly widely used static program analysis technique transforms a given program into a set of logical formulae (verification conditions) and attempts to prove them (see e.g. [9]). When the program involves numeric values (rationals, integers, reals), one way of proving the conditions is logical reasoning. This is usually inefficient because such proofs would need to start from the "bare" axioms of the underlying numerical domains. One way to alleviate the difficulty is to combine logical reasoning with algebraic techniques (algorithms based on deep knowledge about the numerical domains). This approach turns out to be more successful than the pure logical approach. Unfortunately one cannot yet verify even moderate sized programs, mainly because the quantifier elimination methods are in general very expensive (doubly exponential in the number of variables) [6]. Fortunately, our previous experience with the approach provided us with the following observations:

- The verification conditions can be often simplified before applying the quantifier elimination methods on them.

- The verification conditions often have certain interesting structures, which may be exploited by using special versions of the algebraic algorithms.

These observations also hold for the research presented in this paper, namely proving partial correctness of imperative loops and algorithm optimization.

Therefore was necessary to:

1. develop a systematic method to simplify the verification conditions into the forms that makes the quantifier elimination methods more efficient (*Section 3*).

2. use algebraic algorithms suitable to the specific structure of the verification conditions which often occur in program verification (*Section 2*).

In the following, we present a motivating example for the problems addressed in this paper.

Consider the algorithm for computing the square root of a real number (*Algorithm 1*).

Given the loop invariant $I(a,b,x) \iff 0 < a \leq \sqrt{x} \leq b$ and the termination term $d(a,b) := b - a$, we are interested in:

Algorithm 1 Computing the square root of a real number

```
in: $x$: $x > 1$;
    $\varepsilon$: $\varepsilon > 0$
out: $a,b$: $a \geq 0 \wedge b \geq 0 \wedge a \leq \sqrt{x} \leq b \wedge b - a \leq \varepsilon$
$a := 1; b := x$;
while $(b - a > \varepsilon)$ do
    $a := \frac{ab+x}{a+b}$; $b := \frac{b^2+x}{2b}$;
return $a,b$
```

1. proving the correctness of the algorithm;
2. synthesizing an algorithm which terminates faster than the given one and fulfils the same specification (provided that such an algorithm exists).

The following verification conditions are generated using a calculus based on forward symbolic execution and functional semantics [9]:

1. partial correctness

   (a)

   $$\underset{x,\varepsilon}{\forall}\, x > 1 \wedge \varepsilon > 0 \Longrightarrow x > 0 \wedge 0 < 1 \leq x \leq x^2$$

   (b)

   $$\underset{a,b,x,\varepsilon}{\forall}\, 0 < a^2 \leq x \leq b^2 \wedge b - a > \varepsilon \Longrightarrow 0 < (\frac{ab+x}{a+b})^2 \leq x \leq (\frac{b^2+x}{2b})^2 \qquad (1)$$

   (c)

   $$\underset{a,b,x,\varepsilon}{\forall}\, 0 < a^2 \leq x \leq b^2 \wedge b - a \leq \varepsilon \Longrightarrow 0 < a^2 \leq x \leq b^2 \wedge b - a \leq \varepsilon$$

2. termination

   $$\underset{c\in(0,1)}{\exists}\underset{a,b,x}{\forall}\, I(a,b,c) \Longrightarrow d \circ f(a,b,x) \leq c \cdot d(a,b,x)$$

In order to optimize the algorithm, we have to find the smallest constant c such that:

$$\underset{a,b,x}{\forall}\, I(a,b,x) \Longrightarrow d \circ f(a,b,x) \leq c \cdot d(a,b,x).$$

We used `Reduce` command of Mathematica [22] computer algebra system to solve the quantifier elimination problems above, obtaining that the algorithm is indeed correct and the smallest c is $\frac{1}{2}$.

Can we find a faster algorithm having the same specification and b has the form $\frac{pa^2+qab+rb^2}{a+b}$? To answer this question one has to find the parameters p,q,r such that the new algorithm is optimal. To achieve this, firstly, we have to find the necessary and sufficient conditions such that (2) holds. In other words, we have to solve the following quantifier elimination problem:

$$\underset{a,b,x}{\forall}\, 0 < a^2 \leq x \leq b^2 \Longrightarrow 0 < (\frac{ab+x}{a+b})^2 \leq x \leq (\frac{pa^2+qab+rb^2x}{a+b})^2. \qquad (2)$$

The problem can be solved theoretically by quantifier elimination by cylindrical algebraic decomposition. The original algorithm is due to G. Collins [4]. Many improvements of the algorithm exists [11, 3] but the algorithm is intrinsically doubly exponential [6] which makes impossible to handle yet moderate size problems, like (2). To solve the problem: *i*) we carried out manually quantifier elimination for (2) by choosing different values for the parameter q, *ii*) we obtained formulas in p and r from which we could deduce a common pattern, *iii*) finally, we combined the steps above obtaining a formula in p,q,r equivalent to (2), i. e.:

$$r-\frac{1}{4}\geq 0\wedge\left[\begin{array}{l}\left[q-\frac{1}{2}\leq 0\wedge p-2q+r+\frac{1}{2}\geq 0\right]\\ \vee\\ \left[\begin{array}{l}q-\frac{1}{2}>0\wedge\\ \left[\begin{array}{l}p-q+\frac{1}{4}\leq 0\wedge p-2q+r+\frac{1}{2}\geq 0\\ \vee\\ p-q+\frac{1}{4}>0\wedge(p-\frac{1}{4})\cdot(r-\frac{1}{4})\geq(q-\frac{1}{2})^2\end{array}\right]\end{array}\right]\end{array}\right] \tag{3}$$

¿From here, we obtain $p=\frac{1}{4}$, $q=\frac{1}{2}$, $r=\frac{1}{4}$ as the values for the optimized loop.
Indeed, the new synthesized algorithm converges faster, namely the smallest c is $\frac{1}{4}$.

The above example gives us the motivation to study more general problems, namely:

1. ***Problem* 1.** Can we prove/disprove efficiently the inductiveness of the invariant (formulas of type (1)) in case of arbitrary polynomials standing for the loop invariant and variable assignments?

2. ***Problem* 2.** Can we synthesize the fastest terminating algorithm for *Algorithm 1* in case of general assignments, i. e. $a:=\frac{pa^2+qab+rb^2}{sa+tb}$ and $b:=\frac{\alpha a^2+\beta ab+\gamma b^2}{\mu a+\nu b}$?

Our way to approach these problems is presented in *Section 2 and 3*.

1.1 Research Time Frame

The research presented in this activity report was realized as follows:

- January, 2011: literature survey and familiarization with the software for quantifier elimination (QEPCAD-B [1], Redlog [8] and Mathematica [22]).

- February, 2011: work on proving the partial correctness of imperative loops (*Section 2*).

- March - May, 2011: work on the optimization of algorithms (*Section 3*, including the motivating example presented in the *Introduction*).

1.2 Related Work

Applying symbolic computation methods to program verification is a relatively new research area.
Existing work is on the following directions:

- invariant generation, by combining methods like Gröbner bases, Cylindrical Algebraic Decomposition, symbolic summation, recurrence solving and generating functions [12, 13, 19, 20].

- proving the correctness of imperative programs, by using Gröbner bases, Cylindrical Algebraic Decomposition [7, 17].

However, we are not aware of related work applying the symbolic computation methods from our research agenda to program analysis.

In the area of symbolic computation, efficient resultant computation of composed polynomials was studied in [16]. Efficient resultant computation by polynomial interpolation was used to find the implicit equation of rational curves and surfaces [15]. We are not aware of methods for proving verification conditions using the method proposed by us, namely taking into consideration the special structure of some verification conditions, namely those proving the inductiveness of the invariant. They have the special structure: $\underset{x}{\forall} I(x) = 0 \Longrightarrow I(f(x)) = 0$. There exists work exploiting the polynomial formulas in the pure $\forall$ fragment by combining Gröbner Bases computation with semidefinite programming for the real Nullstellensatz [18] or by using sum of squares technique [10]. Contrary to these, our method is currently applied to univariate polynomials.

Regarding the second problem, we are aware of program synthesis methods based on logical reasoning, e.g. induction [2]. Unlike these, our method is based on algebraic reasoning and the particular problem we want to solve (approximating the square root of a real number) is interesting for the interval analysis community and gives new challenging problems to state-of-the-art software [1, 22] for quantifier elimination by cylindrical algebraic decomposition.

2 Proving Partial Correctness of Imperative Loops

Let $K[x]$ be a polynomial ring in one variable. Consider the following loop, where the loop condition is ignored, annotated with a polynomial invariant $g(x) = 0$, $g \in K[x]$.

Algorithm 2 Simple loop

```
while (?) do
    $x := f(x);$
```

We are interested in solving the following problem. *Given an imperative loop annotated with a formula that it is claimed to be its invariant, decide whether the claim is correct.* This problem can be viewed also as a polynomial algebra problem and consequently powerful techniques and algorithms belonging to this area of mathematics can be applied to solve it.

Denoting by $g(x) = 0$ the polynomial standing for the loop invariant and by $f(x)$ the polynomial standing for the assignment of the loop variable[1], the problem specification in the algebraic setting is as follows. *Given the polynomials $f, g \in K[x]$, check efficiently whether g and $g \circ f$ have common solutions.*

In the following, we introduce the notion of resultant and establish the relationship between the resultant of two polynomials and their common solutions. We follow [5].

Definition 1. *Given polynomials $f, g \in K[x]$ of positive degree, write them in the form*

$$f = a_l x^l + \ldots + a_0,\ a_l \neq 0,$$
$$g = b_m x^m + \ldots + b_0,\ b_m \neq 0.$$

Then the Sylvester matrix of f and g with respect to x, denoted $Syl(f,g,x)$, is the following $(l+m) \times (l+m)$ matrix of coefficients of f and g:

[1] As a starting point and preliminary study, the univariate case is considered; an univariate polynomial standing for the loop invariant and for variable assignment is considered

$$Syl(f,g,x) = \begin{pmatrix} a_l & & \cdots & & a_0 & 0 & 0 & 0 \\ 0 & a_l & & \cdots & & a_0 & 0 & 0 \\ 0 & 0 & \ddots & & & & \ddots & 0 \\ 0 & 0 & 0 & a_l & & \cdots & & a_0 \\ b_m & & \cdots & & b_0 & 0 & 0 & 0 \\ 0 & b_m & & \cdots & & b_0 & 0 & 0 \\ 0 & 0 & \ddots & & & & \ddots & 0 \\ 0 & 0 & 0 & b_m & & \cdots & & b_0 \end{pmatrix}$$

The resultant of f and g with respect to x, denoted by $Res(f,g,x)$, is the determinant of the Sylvester matrix, i.e. $Res(f,g,x) = det(Syl(f,g,x))$.

Theorem 1. *Given $f,g \in K[x]$ of positive degree, the resultant $Res(f,g,x) \in K$ is an integer polynomial in the coefficients of f and g. Furthermore, f and g have a common factor in $K[x]$ iff $Res(f,g,x) = 0$.*

Given the results in *Theorem 1*, we approached our problem as follows:

1. Compute the resultant of $g(x)$ and $g(f(x))$, by expanding $g(f(x))$.
2. Compute the resultant of $g(x)$ and $g(y)$, where $y = f(x)$.

However, one can observe the large dimension of $Syl(f,g,x)$, namely $(l+m)\times(l+m)$, whose determinant has to be computed, as well as the similar structure of $g(x)$ and $g(f(x))$. The following questions naturally occur. Is there another type of matrix, with lower dimension, from which we can determine the common factors of two polynomials? Can we exploit the structure of $g(f(x))$? The answer is yes, the *Bézout matrix* can be used at this aim.

In the following, we define the Bézout matrix and establish the relationship between the Bézoutian of two polynomials and their common solutions. We follow [14].

Given two polynomials f,g, assume, without loss of generality, that they have the degree l.

Definition 2. *The expression* $h(x,y) = \dfrac{\begin{vmatrix} f(x) & f(y) \\ g(x) & g(y) \end{vmatrix}}{x-y} = \frac{f(x)g(y)-g(x)f(y)}{x-y} = \sum\limits_{i,j=0}^{l} c_{ij}x^iy^j$ *is a polynomial in* $K[x,y]$*. Then the matrix* $B(f,g) = \left[c_{i,j}\right]_{i,j=0}^{l}$ *is called the Bézout matrix associated to the polynomials f and g.*

Theorem 2. *The polynomials f and g have common a common factor iff the associated Bézout matrix $B(f,g)$ is singular.*

Given the above facts, we propose a third method for verifying whether two polynomials g and $g \circ f$ have a common solution. It is based on Bézoutian matrix and polynomial interpolation.

Definition 3. *Suppose that we are given n points (x_k,y_k), $k = 1,...,n$, with pairwise distinct x_k. Then, there is a unique polynomial, p_{n-1}, of degree $n-1$, which interpolates this data. The Lagrange form of p_{n-1} may be explicitly given by means of the fundamental polynomials or cardinality functions, L_i, defined by:*

$$L_i(x) = \prod_{\substack{k=1 \\ k\neq i}}^{n} \frac{x-x_k}{x_i-x_k}.$$

Remark 1. *For the simplicity of the presentation we exemplify the approach for the polynomials f and g. The fact that we have $g \circ f$ matters only at the step when we evaluate the polynomial at a point. This is done in the case of $g \circ f$ by evaluating f at x and then g at $f(x)$. Both g and $g \circ f$ have the degree of $g \circ f$.*

$$\text{Let } h(x,y) = \frac{\begin{vmatrix} f(x) & f(y) \\ g(x) & g(y) \end{vmatrix}}{x-y} = \frac{f(x)g(y)-g(x)f(y)}{x-y} = \sum_{i,j=0}^{l} c_{ij}x^iy^j = \begin{pmatrix} 1 & x & \cdots & x^l \end{pmatrix} \begin{pmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,l} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,l} \\ \vdots & \vdots & \ddots & \vdots \\ c_{l,0} & c_{l,1} & \cdots & c_{l,l} \end{pmatrix} \begin{pmatrix} 1 \\ y \\ \vdots \\ y^l \end{pmatrix}.$$

Another way of expressing $h(x,y)$ is by means of Lagrange bivariate interpolation.

We consider the interpolation points (x_i,y_j), $(i,j = 0,...,l)$ and the interpolation space $\mathscr{S}_{l,l}(x,y)$.

The interpolation problem is stated as follows. Given $l \cdot l$ values $h_{ij} \in K$ (interpolation data), find a polynomial $h(x,y) = \sum\limits_{i,j=0}^{l} c_{ij}x^iy^j \in \mathscr{S}_{l,l}(x,y)$ such that $h(x_i,y_j) = h_{ij}$, for all $(i,j) \in I$. We consider for the interpolation space $\mathscr{S}_{l,l}(x,y)$ the basis $\{1,y,\cdots,y^l,x,xy,\cdots,xy^l,\cdots,x^l,x^ly,\cdots,x^ly^l\}$, and the interpolation points in the order: $(x_0,y_0),(x_0,y_1),\cdots,(x_0,y_l),\cdots,(x_l,y_0),\cdots,(x_l,y_l)$. Then the $l \cdot l$ interpolation conditions $h(x_i,y_j) = h_{ij}$ can be written as

$$H = V_x C V_y, \tag{4}$$

where $H = (h_{ij})_{i,j=0}^{l}$, $C = (c_{ij})_{i,j=0}^{l}$, V_x and V_y are Vandermonde matrices defined as:

$$V_x = \begin{pmatrix} 1 & x_0 & \cdots & x_0^l \\ 1 & x_1 & \cdots & x_1^l \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_l & \cdots & x_l^l \end{pmatrix} \qquad V_y = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ y_0 & y_1 & \cdots & y_l \\ \vdots & \vdots & \ddots & \vdots \\ y_0^l & y_1^l & \cdots & y_l^l \end{pmatrix}$$

Remark 2. *One could also compute the entries of the matrix C, $C = V_x^T H V_y^T$. However, for our purpose this is not necessary.*

One can take $Det(H) = Det(V_x C V_y) = Det(V_x)Det(C)Det(V_y)$. C is singular iff H is singular, provided that V_x and V_y are nonsingular. Moreover, for simplifying the entries of the matrix H, the denominator of $h(x,y)$ can be omitted because it does not influences the fact that the determinant of H is zero or not. However, when choosing the interpolation points (x_i,y_j) we have to ensure simultaneously the following:

1. the entries of V_x and V_y, respectively, must be pairwise distinct, in order V_x and V_y to be nonsingular.
2. the denominators of $h(x_i,y_i)$ do not vanish. The values of $h(x_i,y_i)$ $(i,j = 1,...,l)$ fill the matrix H.
3. the polynomials f and g have high degree and have to be evaluated at these points.

The following experiments have shown that the way the interpolation points x_i and y_j are chosen is crucial for the speed of the method.

1. Methods for computing x_i and y_j using additional operations are costly (e.g. division, square root).
2. Numerical approximations of the operations above lead to probabilistic algorithms, which are not completely accurate.

Table 1: Experimental Results

Method 1	Method 2	Method 3	$(n,p,d,minC,maxC)$
0.00125	0.00188	0.00016	$(100,6,5,-9,9)$
0.00266	0.00281	$8.60314*10^{-18}$	$(100,8,7,-9,9)$
0.01093	0.00562	$2.40671*10^{-17}$	$(100,11,10,-9,9)$
0.02516	0.0078	$2.55416*10^{-17}$	$(100,13,12,-9,9)$
0.07328	0.01376	$2.50051*10^{-16}$	$(100,18,17,-9,9)$
0.1414	0.01812	$2.72715*10^{-16}$	$(100,21,20,-9,9)$
0.32719	0.02627	$2.17603*10^{-16}$	$(100,23,22,-9,9)$
0.51047	0.03452	0.00015	$(100,25,24,-9,9)$

3. Evaluating arbitrary polynomials at a large number is computationally expensive.

With these in mind, we generated randomly real values in the interval $[0,1]$ for x_i and y_j, $i,j=0,\cdots,l$.

Therefore, checking whether f and g have common solution reduces to the following:

1. compute the entries of the matrix H.

2. check whether H is singular. H is singular iff f and g have common solutions.

We implemented in Mathematica computer algebra system [22] and compared the average computing time of the three methods. The performance of the methods was tested on sets of 100 dense univariate polynomials, with degree up to 25 and coefficients in the interval $[-9, 9]$. The results of the experiments are presented in *Table 2*. Methods 1, 2 and 3 represent, in this order: the computation of the resultant by expansion, the computation of the resultant by denoting $y=f(x)$, and the computation of the determinant of the Bézout matrix using polynomial interpolation. n represents the number of test polynomials, p represents the number of power products of a polynomial, d its degree, *minC* and *maxC* the minimum and, respectively, its maximum coefficient. The numbers in the first three columns represent seconds.

We observe that the method proposed by us (Method 3) outperforms the others.

3 Algorithm Optimization

We are interested in solving the following problem.

Given *Algorithm 3*, find the parameters $p,q,r,s,t,\alpha,\beta,\gamma,\mu,\nu$ such that the difference $U(\alpha)-L(p)$, where $U(\alpha)=\frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b}$ and $L(p)=\frac{pa^2+qab+rb^2+x}{sa+tb}$, is minimal.

Algorithm 3 Computing $\sqrt{x}$ (general polynomial assignments)

```
in: $x$: $x>1$;
    $\varepsilon$: $\varepsilon>0$
out: $a,b$: $a \le \sqrt{x} \le b \wedge b-a \le \varepsilon$
$a:=1; b:=x$;
while $(b-a>\varepsilon)$ do
    $a:=\frac{pa^2+qab+rb^2}{sa+tb}$; $b:=\frac{\alpha a^2+\beta ab+\gamma b^2}{\mu a+\nu b}$;
return $a,b$
```

Denoting by $I(a,b) \iff 0 < a \leq \sqrt{x} \leq b$ the loop invariant, $d(a,b) := b - a$ the termination term, $f(p,\alpha) = (\frac{pa^2+qab+rb^2}{sa+tb}, \frac{\alpha a^2+\beta ab+\gamma b^2}{\mu a+\nu b})$ the loop assignments, the above problem is an optimization problem, which and can be formulated in two ways:

1. Find $p,q,r,s,t,\alpha,\beta,\gamma,\mu,\nu$ such that $\underset{\substack{p\prime,\ldots,t\prime \\ \alpha\prime,\ldots,\nu\prime}}{\forall} \underset{a,b,x}{\forall} I(a,b) \Longrightarrow (d \circ f(p\prime,\alpha\prime) \geq d \circ f(p,\alpha))$.

2. Find the smallest c such that $\underset{a,b,x}{\forall} I(a,b) \Longrightarrow (d \circ f(p,\alpha) \leq c \cdot d(a,b))$.

Note that the first formulation is stronger than the second one and it could be possible that witnesses for the parameters can not be found.

A preliminary task in the optimization problem is to find the necessary and sufficient conditions such that the invariant is inductive, i.e. find the conditions on the parameters $p,q,r,s,t,\alpha,\beta,\gamma,\mu,\nu$ such that the following formula holds:

$$\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Longrightarrow 0 < \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \leq \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b}. \tag{5}$$

which is equivalent to:
$\big[\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} > 0\big] \wedge \big[\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x}\big] \wedge$
$\big[\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x}\big]$.

We found the necessary and sufficient conditions by carrying out equivalent transformation of the three formulas following the next steps.

1. We considered all possible sign combinations on the parameters occurring in the denominators (s, t, μ, and ν).

2. We found the quantifier-free formula equivalent to the given one.

The step 2 above can be solved, in principle, automatically by using a software specialized in quantifier elimination. We have used QEPCAD-B [1], `Reduce` command of Mathematica [22] and Redlog [8]. The first two are state-of-the-art software for quantifier elimination by cylindrical algebraic decomposition. Redlog implements virtual substitution method [21]. QEPCAD-B and Mathematica could not handle our formulas involving non-linear inequalities with 8 variable (of which 5 were free). Redlog, which is actually specialized in handling formulas with degree at most 2 of the quantified variables, output a quantifier-free formula equivalent to the given one, but the formula is very long and hard to be interpreted and used further in the optimization. Therefore:

- we have eliminated manually an universally quantified variable,

- we have found automatically, using QEPCAD-B, the quantifier-free formula equivalent to the new one, which was possible in most of the cases. However, for the formula $0 < a \leq \frac{\mu a+\nu b}{2} \leq b \Rightarrow -(\frac{\mu a+\nu b}{2})^2 + \alpha a^2 + \beta ab + \gamma b^2 \geq 0$ with $\mu > 0$ and $\nu > 0$ (*Lemma 3*, Case 3.1) two equivalent quantifier-free formula were found. One was found semi-automatically, namely we divided the formula into simpler ones which could be handled by QEPCAD-B and then combine the results. The other was found automatically using Redlog.

In the following, we present the derivation of the necessary and sufficient conditions for (5). We do not give all the details of the proofs of the lemmas to avoid repetition. However, we plan to include them in a technical report which will be available at `http://www.risc.jku.at/publications/`.

Lemma 1. *Prove that:* $\underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} > 0 \Longleftrightarrow$

$$\left[\begin{array}{l} [\; r \geq 0 \quad\quad \wedge t \geq 0 \wedge s+t > 0 \wedge (p+1)+q+r > 0 \wedge [q \geq 0 \vee 2(p+1)+q < 0 \vee 4(p+1)r-q^2 > 0 \;] \\ \bigvee \\ [\; r+1 \leq 0 \wedge t \leq 0 \wedge s+t < 0 \wedge p+q+(r+1) < 0 \wedge [q \leq 0 \vee 2p+q > 0 \quad\quad \vee 4p(r+1)-q^2 > 0] \;] \end{array}\right].$$

Proof. $\underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} > 0 \Longleftrightarrow$

$\underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0.$

In the following we proceed by equivalent transformations by considering all possible cases for s and t.

1.1 Case $s > 0 \wedge t > 0$.

$$\begin{array}{l} \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x > 0 \overset{(4)}{\Longleftrightarrow} \\ \underset{a,b}{\forall}\, 0 < a \leq b \qquad\quad \Rightarrow (p+1)a^2+qab+rb^2 > 0. \end{array}$$

The last formula is handled by a quantifier elimination software, namely QEPCAD-B, obtaining the quantifier-free formula:

$r \geq 0 \wedge (p+1)+q+r > 0 \wedge \left[q \geq 0 \vee 2(p+1)+q < 0 \vee 4(p+1)r-q^2 > 0\right].$

1.2 Case $s < 0 \wedge t < 0$.

$$\begin{array}{l} \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x < 0 \overset{(5)}{\Longleftrightarrow} \\ \underset{a,b}{\forall}\, 0 < a \leq b \qquad\quad \Rightarrow (r+1)b^2+qab+pa^2 < 0. \end{array}$$

The last formula is handled by a quantifier elimination software, namely QEPCAD-B, obtaining the quantifier-free formula:

$r+1 \leq 0 \wedge p+q+(r+1) < 0 \wedge \left[q \leq 0 \vee 2p+q > 0 \vee 4p(r+1)-q^2 > 0\right].$

1.3 Case $s > 0 \wedge t < 0 \wedge s+t = 0$.

$$\begin{array}{l} \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \overset{(6)}{\Longleftrightarrow} \\ false. \end{array}$$

1.4 Case $s > 0 \wedge t < 0 \wedge s+t > 0$.

$$\begin{array}{l} \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ false. \end{array}$$

1.5 Case $s > 0 \wedge t < 0 \wedge s+t < 0$.

$$\begin{array}{l} \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \overset{(7)}{\Longleftrightarrow} \\ \underset{a,b,x}{\forall}\, 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x < 0 \Longleftrightarrow \\ \underset{a,b}{\forall}\, 0 < a \leq b \qquad\quad \Rightarrow (r+1)b^2+qab+pa^2 < 0 \Longleftrightarrow \\ r+1 \leq 0 \wedge p+q+(r+1) < 0 \wedge \left[q \leq 0 \vee 2p+q > 0 \vee 4p(r+1)-q^2 > 0\right]. \end{array}$$

1.6 Case $s < 0 \wedge t > 0 \wedge s+t = 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ false.\end{array}$$

1.7 Case $s < 0 \wedge t > 0 \wedge s+t < 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ false.\end{array}$$

1.8 Case $s < 0 \wedge t > 0 \wedge s+t > 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x > 0 \Longleftrightarrow \\ \underset{a,b}{\forall}\ \ 0 < a \leq b \qquad\quad \Rightarrow (p+1)a^2+qab+rb^2 > 0 \Longleftrightarrow \\ r \geq 0 \wedge (p+1)+q+r > 0 \wedge \left[q \geq 0 \vee 2(p+1)+q < 0 \vee 4(p+1)r-q^2 > 0\right].\end{array}$$

1.9 Case $s > 0 \wedge t = 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x > 0 \Longleftrightarrow \\ \underset{a,b}{\forall}\ \ 0 < a \leq b \qquad\quad \Rightarrow (p+1)a^2+qab+rb^2 > 0 \Longleftrightarrow \\ r \geq 0 \wedge (p+1)+q+r > 0 \wedge \left[q \geq 0 \vee 2(p+1)+q < 0 \vee 4(p+1)r-q^2 > 0\right].\end{array}$$

1.10 Case $s = 0 \wedge t > 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x > 0 \Longleftrightarrow \\ \underset{a,b}{\forall}\ \ 0 < a \leq b \qquad\quad \Rightarrow (p+1)a^2+qab+rb^2 > 0 \Longleftrightarrow \\ r \geq 0 \wedge (p+1)+q+r > 0 \wedge \left[q \geq 0 \vee 2(p+1)+q < 0 \vee 4(p+1)r-q^2 > 0\right].\end{array}$$

1.11 Case $s = 0 \wedge t < 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x < 0 \Longleftrightarrow \\ \underset{a,b}{\forall}\ \ 0 < a \leq b \qquad\quad \Rightarrow (r+1)b^2+qab+pa^2 < 0 \Longleftrightarrow \\ r+1 \leq 0 \wedge p+q+(r+1) < 0 \wedge \left[q \leq 0 \vee 2p+q > 0 \vee 4p(r+1)-q^2 > 0\right]..\end{array}$$

1.12 Case $s < 0 \wedge t = 0$.

$$\begin{array}{l}\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb) > 0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x < 0 \Longleftrightarrow \\ \underset{a,b}{\forall}\ \ 0 < a \leq b \qquad\quad \Rightarrow (r+1)b^2+qab+pa^2 < 0 \Longleftrightarrow \\ r+1 \leq 0 \wedge p+q+(r+1) < 0 \wedge \left[q \leq 0 \vee 2p+q > 0 \vee 4p(r+1)-q^2 > 0\right].\end{array}$$

Summarizing we have:

$$
\begin{array}{l}
\left[\begin{array}{l}
\big[(s>0\wedge t>0)\vee(s<0\wedge t>0\wedge s+t>0)\vee(s>0\wedge t=0)\vee(s=0\wedge t>0)\big]\Longrightarrow\\
\quad\left[\begin{array}{l}
\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{pa^2+qab+rb^2+x}{sa+tb}>0\Longleftrightarrow\\
r\ge 0\qquad\wedge(p+1)+q+r>0\wedge\big[q\ge 0\vee 2(p+1)+q<0\vee 4r(p+1)-q^2>0\big]
\end{array}\right]
\end{array}\right]\\
\wedge\\
\left[\begin{array}{l}
\big[(s<0\wedge t<0)\vee(s>0\wedge t<0\wedge s+t<0)\vee(s=0\wedge t<0)\vee(s<0\wedge t=0)\big]\Longrightarrow\\
\quad\left[\begin{array}{l}
\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{pa^2+qab+rb^2+x}{sa+tb}>0\Longleftrightarrow\\
r+1\le 0\wedge p+q+(r+1)<0\wedge\big[q\le 0\vee 2p+q>0\quad\vee 4p(r+1)-q^2>0\big]
\end{array}\right]
\end{array}\right]\\
\Longleftrightarrow\\
\left[\begin{array}{l}
\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{pa^2+qab+rb^2+x}{sa+tb}>0\Longleftrightarrow\\
\quad\left[\begin{array}{l}
\big[\ r\ge 0\qquad\wedge t\ge 0\wedge s+t>0\wedge(p+1)+q+r>0\wedge\big[q\ge 0\vee 2(p+1)+q<0\vee 4(p+1)r-q^2>0\big]\ \big]\\
\vee\\
\big[\ r+1\le 0\wedge t\le 0\wedge s+t<0\wedge p+q+(r+1)<0\wedge\big[q\le 0\vee 2p+q>0\qquad\vee 4p(r+1)-q^2>0\big]\ \big]
\end{array}\right]
\end{array}\right].
\end{array}
$$

□

Lemma 2. *Prove that:* $\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{pa^2+qab+rb^2+x}{sa+tb}\le\sqrt{x}\Longleftrightarrow$

$$
\left[\begin{array}{l}
\left[\begin{array}{l}
r\le 0\wedge t\ge 0\wedge s+t>0\wedge t-r-1\ge 0\wedge t+s-p-q-1\ge 0\wedge\\
\big[t-q>0\vee r+(s-p-1)<0\vee 4r(s-p-1)+(t-q)^2\le 0\big]\wedge\\
\big[s-q>0\vee s-q-2p<0\qquad\vee 4p(t-r-1)+(s-q)^2\le 0\big]
\end{array}\right]\\
\bigvee\\
\left[\begin{array}{l}
r\ge 0\wedge t\le 0\wedge s+t<0\wedge t-r-1\le 0\wedge t+s-p-q-1\le 0\wedge\\
\big[t-q<0\vee r+(s-p-1)>0\vee 4r(s-p-1)+(t-q)^2\le 0\big]\wedge\\
\big[s-q<0\vee s-q-2p>0\qquad\vee 4p(t-r-1)+(s-q)^2\le 0\big]
\end{array}\right]
\end{array}\right].
$$

Proof.

2.1 Case $s>0\wedge t>0$.

$$
\begin{array}{l}
\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{pa^2+qab+rb^2+x}{sa+tb}\le\sqrt{x}\Longleftrightarrow\\
\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow pa^2+qab+rb^2+x\le\sqrt{x}(sa+tb)\Longleftrightarrow\\
\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow x-\sqrt{x}(sa+tb)+pa^2+qab+rb^2\le 0\overset{(8)}{\Longleftrightarrow}\\
\underset{a,b}{\forall}\ \ 0<a\le b\qquad\Rightarrow\left[\begin{array}{l}
a^2-a(sa+tb)+pa^2+qab+rb^2\le 0\\
\wedge\\
b^2-b(sa+tb)+pa^2+qab+rb^2\le 0
\end{array}\right]\Longleftrightarrow\\
\left[\begin{array}{l}
\underset{a,b}{\forall}\ \ 0<a\le b\quad\Rightarrow a^2-a(sa+tb)+pa^2+qab+rb^2\le 0\\
\wedge\\
\underset{a,b}{\forall}\ \ 0<a\le b\quad\Rightarrow b^2-b(sa+tb)+pa^2+qab+rb^2\le 0
\end{array}\right].
\end{array}
$$

The last formulas are handled by a quantifier elimination software, namely QEPCAD-B. After simplification we obtain:

$$
\begin{array}{l}
r\le 0\wedge t-r-1\ge 0\wedge t+s-p-q-r-1\ge 0\wedge\\
\big[t-q>0\vee r+(s-p-1)<0\vee 4r(s-p-1)+(t-q)^2\le 0\big]\wedge\\
\big[s-q>0\vee s-q-2p<0\qquad\vee 4p(t-r-1)+(s-q)^2\le 0\big].
\end{array}
$$

2.2 Case $s<0\wedge t<0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow \\
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow pa^2+qab+rb^2+x \geq \sqrt{x}(sa+tb) \Longleftrightarrow \\
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow x - \sqrt{x}(sa+tb) + pa^2+qab+rb^2 \geq 0 \overset{(9)}{\Longleftrightarrow} \\
\left[\begin{array}{ll}
\underset{a,b}{\forall} a \leq \frac{sa+tb}{2} \leq b \Rightarrow [0 < a \leq b \Rightarrow -(\frac{sa+tb}{2})^2 + pa^2+qab+rb^2 \geq 0] & \\
\wedge & \\
\underset{a,b}{\forall} & 0 < a \leq b \Rightarrow a^2 - a(sa+tb) + pa^2+qab+rb^2 \geq 0 \\
\wedge & \\
\underset{a,b}{\forall} & 0 < a \leq b \Rightarrow b^2 - b(sa+tb) + pa^2+qab+rb^2 \geq 0
\end{array}\right] \Longleftrightarrow \\
\left[\begin{array}{ll}
\underset{a,b}{\forall} 0 < a \leq \frac{sa+tb}{2} \leq b \Rightarrow -(\frac{sa+tb}{2})^2 + pa^2+qab+rb^2 \geq 0 & \\
\wedge & \\
\underset{a,b}{\forall} & 0 < a \leq b \Rightarrow a^2 - a(sa+tb) + pa^2+qab+rb^2 \geq 0 \\
\wedge & \\
\underset{a,b}{\forall} & 0 < a \leq b \Rightarrow b^2 - b(sa+tb) + pa^2+qab+rb^2 \geq 0
\end{array}\right] \overset{(10)}{\Longleftrightarrow} \\
\left[\begin{array}{l}
\underset{a,b}{\forall} 0 < a \leq b \Rightarrow a^2 - a(sa+tb) + pa^2+qab+rb^2 \leq 0 \\
\wedge \\
\underset{a,b}{\forall} 0 < a \leq b \Rightarrow b^2 - b(sa+tb) + pa^2+qab+rb^2 \leq 0
\end{array}\right].
\end{array}$$

The last formulas are handled by a quantifier elimination software, namely QEPCAD-B. After simplification we obtain:

$$\begin{array}{l}
r \geq 0 \wedge t - r - 1 \leq 0 \wedge t + s - p - q - r - 1 \leq 0 \wedge \\
\left[t - q < 0 \vee r + (s - p - 1) > 0 \vee 4r(s-p-1) + (t-q)^2 \leq 0\right] \wedge \\
\left[s - q < 0 \vee s - q - 2p > 0 \qquad \vee 4p(t-r-1) + (s-q)^2 \leq 0\right].
\end{array}$$

2.3 Case $s > 0 \wedge t < 0 \wedge s + t = 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \overset{(11)}{\Longleftrightarrow} \\
\left[\begin{array}{l}
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \wedge sa+tb < 0 \Rightarrow pa^2+qab+rb^2+x \geq \sqrt{x}(sa+tb) \\
\wedge \\
\underset{a,b,x}{\forall} \neg(0 < a \leq \sqrt{x} \leq b \wedge sa+tb = 0)
\end{array}\right] \overset{(12)}{\Longleftrightarrow} \\
\left[\begin{array}{l}
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \wedge sa+tb < 0 \Rightarrow pa^2+qab+rb^2+x \geq \sqrt{x}(sa+tb) \\
\wedge \\
false
\end{array}\right] \Longleftrightarrow \\
false.
\end{array}$$

2.4 Case $s > 0 \wedge t < 0 \wedge s + t > 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow \\
false.
\end{array}$$

2.5 Case $s > 0 \wedge t < 0 \wedge s + t < 0$.

$$\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$

$$\left[\begin{array}{l} r \geq 0 \wedge t-r-1 \leq 0 \wedge t+s-p-q-r-1 \leq 0 \wedge \\ \left[t-q<0 \vee r+(s-p-1)>0 \vee 4r(s-p-1)+(t-q)^2 \leq 0\right] \wedge \\ \left[s-q<0 \vee s-q-2p>0 \quad \vee \quad 4p(t-r-1)+(s-q)^2 \leq 0\right] \end{array}\right].$$

2.6 Case $s<0 \wedge t>0 \wedge s+t=0$.

$$\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$
false.

2.7 Case $s<0 \wedge t>0 \wedge s+t<0$.

$$\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$
false.

2.8 Case $s<0 \wedge t>0 \wedge s+t>0$.

$$\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$
$$\left[\begin{array}{l} r \leq 0 \wedge t-r-1 \geq 0 \wedge t+s-p-q-r-1 \geq 0 \wedge \\ \left[t-q>0 \vee r+(s-p-1)<0 \vee 4r(s-p-1)+(t-q)^2 \leq 0\right] \wedge \\ \left[s-q>0 \vee s-q-2p<0 \qquad \vee 4p(t-r-1)+(s-q)^2 \leq 0\right] \end{array}\right].$$

2.9 Case $s>0 \wedge t=0$.

$$\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$
$$\left[\begin{array}{l} r \leq 0 \wedge t-r-1 \geq 0 \wedge t+s-p-q-r-1 \geq 0 \wedge \\ \left[t-q>0 \vee r+(s-p-1)<0 \vee 4r(s-p-1)+(t-q)^2 \leq 0\right] \wedge \\ \left[s-q>0 \vee s-q-2p<0 \qquad \vee 4p(t-r-1)+(s-q)^2 \leq 0\right] \end{array}\right].$$

2.10 Case $s=0 \wedge t>0$.

$$\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$
$$\left[\begin{array}{l} r \leq 0 \wedge t-r-1 \geq 0 \wedge t+s-p-q-r-1 \geq 0 \wedge \\ \left[t-q>0 \vee r+(s-p-1)<0 \vee 4r(s-p-1)+(t-q)^2 \leq 0\right] \wedge \\ \left[s-q>0 \vee s-q-2p<0 \quad \vee \quad 4p(t-r-1)+(s-q)^2 \leq 0\right] \end{array}\right].$$

2.11 Case $s=0 \wedge t<0$.

$$\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$$
$$\left[\begin{array}{l} r \geq 0 \wedge t-r-1 \leq 0 \wedge t+s-p-q-r-1 \leq 0 \wedge \\ \left[t-q<0 \vee r+(s-p-1)>0 \vee 4r(s-p-1)+(t-q)^2 \leq 0\right] \wedge \\ \left[s-q<0 \vee s-q-2p>0 \quad \vee \quad 4p(t-r-1)+(s-q)^2 \leq 0\right] \end{array}\right].$$

2.12 Case $s<0 \wedge t=0$. $\underset{a,b,x}{\forall} 0<a \leq \sqrt{x} \leq b \Rightarrow \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow$
$$\left[\begin{array}{l} r \geq 0 \wedge t-r-1 \leq 0 \wedge t+s-p-q-r-1 \leq 0 \wedge \\ \left[t-q<0 \vee r+(s-p-1)>0 \vee 4r(s-p-1)+(t-q)^2 \leq 0\right] \wedge \\ \left[s-q<0 \vee s-q-2p>0 \quad \vee \quad 4p(t-r-1)+(s-q)^2 \leq 0\right] \end{array}\right].$$

Summarizing we have:

$$\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{pa^2+qab+rb^2+x}{sa+tb}\le\sqrt{x}\iff$$

$$\left[\begin{array}{l}\left[\begin{array}{l}r\le0\wedge t\ge0\wedge s+t>0\wedge t-r-1\ge0\wedge t+s-p-q-r-1\ge0\wedge\\ \big[t-q>0\vee r+(s-p-1)<0\vee4r(s-p-1)+(t-q)^2\le0\big]\wedge\\ \big[s-q>0\vee s-q-2p<0\qquad\vee4p(t-r-1)+(s-q)^2\le0\big]\end{array}\right]\\ \bigvee\\ \left[\begin{array}{l}r\ge0\wedge t\le0\wedge s+t<0\wedge t-r-1\le0\wedge t+s-p-q-r-1\le0\wedge\\ \big[t-q<0\vee r+(s-p-1)>0\vee4r(s-p-1)+(t-q)^2\le0\big]\ \wedge\\ \big[s-q<0\vee s-q-2p>0\qquad\vee4p(t-r-1)+(s-q)^2\le0\big]\end{array}\right]\end{array}\right].$$

Combining the two lemmas and simplifying, we obtain:

$$\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow0<\frac{pa^2+qab+rb^2+x}{sa+tb}\le\sqrt{x}\iff$$

$$\left[\begin{array}{l}r=0\wedge q\ge0\wedge t-1\ge0\wedge t-q\ge0\wedge s+t>0\wedge p+q+1>0\wedge t+s-p-q-1\ge0\wedge\\ \big[s-q>0\vee s-q-2p<0\vee4p(t-1)+(s-q)^2\le0\big]\end{array}\right].$$

□

Lemma 3. *Prove that:* $\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b}\ge\sqrt{x}\iff$

$$\left[\begin{array}{l}\left[\begin{array}{l}\left[\begin{array}{l}\left[\begin{array}{l}\nu\ge0\wedge\mu+\nu>0\wedge\mu\ge0\wedge\mu-2\le0\wedge\mu+\nu-2=0\wedge4\gamma-\mu^2+4\mu-4\ge0\wedge\alpha+\beta+\gamma-1\ge0\wedge\\ \big[\beta+2\alpha-\mu<0\vee2\beta+\mu^2-2\mu>0\vee4\alpha\gamma-\mu^2\gamma-\beta^2-\mu^2\beta+2\mu\beta-\mu^2\alpha+4\mu\alpha-4\alpha\ge0\big]\end{array}\right]\\ \vee\\ \left[\begin{array}{l}\nu\ge0\wedge\mu+\nu>0\wedge\mu\ge0\wedge\mu-2\le0\wedge\mu+\nu-2\le0\wedge4\gamma-\nu^2\ge0\wedge\\ \mu^2\gamma-4\mu\gamma+4\gamma-\mu\nu\beta+2\nu\beta+\nu^2\alpha-\nu^2\ge0\wedge\\ \big[[\mu-1\le0\wedge\nu-1\le0]\vee4\mu-1\le0\vee4\nu-1\le0\big]\wedge\\ \big[[2\beta-\mu\nu>0\vee\mu\beta-2\beta-2\nu\alpha+\mu\nu>0\vee4\alpha\gamma-\mu^2\gamma-\beta^2+\mu\nu\beta-\nu^2\alpha\ge0\big]\end{array}\right]\\ \vee\\ \left[\begin{array}{l}\nu\ge0\wedge\mu+\nu>0\wedge\mu\ge0\wedge\mu-2\le0\wedge\mu+\nu-2\le0\wedge4\mu-1\le0\wedge\gamma\ge0\wedge\alpha+\beta+\gamma-1\ge0\wedge\\ \big[\beta+2\alpha-2<0\vee\beta>0\vee4\alpha\gamma-4\gamma-\beta^2\ge0\big]\end{array}\right]\end{array}\right.\\ \wedge\\ \gamma\ge0\wedge\alpha+\beta+\gamma-\mu-\nu+1\ge0\wedge\big[\beta-\nu+2(\alpha-\mu+1)<0\vee\beta-\nu>0\vee4\gamma(\alpha-\mu+1)-(\beta-\nu)^2\ge0\big]\\ \wedge\\ \gamma-\nu+1\ge0\wedge\big[\beta+2\alpha-\mu<0\vee\beta-\mu>0\vee4\alpha(\gamma-\nu+1)-(\beta-\mu)^2\ge0\big]\end{array}\right.\\ \bigvee\\ \left[\begin{array}{l}\nu\le0\wedge\mu+\nu<0\wedge\gamma\le0\wedge\gamma-\nu+1\le0\wedge\alpha+\beta+\gamma-\mu-\nu+1\le0\wedge\\ \big[\beta-\nu<0\vee\beta-\nu+2(\alpha-\mu+1)>0\vee4\gamma(\alpha-\mu+1)+(\beta-\nu)^2\ge0\big]\wedge\\ \big[\beta-\mu<0\vee\beta-2\alpha-\mu>0\qquad\qquad\vee4\alpha(\gamma-\nu+1)+(\beta-\mu)^2\ge0\big]\end{array}\right.\end{array}\right.$$

Proof.

3.1 Case $\mu>0\wedge\nu>0$.

$$\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow\frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b}\ge\sqrt{x}\iff$$

$$\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b\Rightarrow x-\sqrt{x}(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2\ge0\iff$$

$$\left[\begin{array}{l}\underset{a,b}{\forall}0<a\le\frac{\mu a+\nu b}{2}\le b\Rightarrow-(\frac{sa+tb}{2})^2+\alpha a^2+\beta ab+\gamma b^2\ge0]\\ \wedge\\ \underset{a,b}{\forall}0<a\le b\Rightarrow a^2-a(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2\ge0\\ \wedge\\ \underset{a,b}{\forall}0<a\le b\Rightarrow b^2-b(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2\ge0\end{array}\right]$$

We obtained automatically the following quantifier-free formulas for the second and third formulas, respectively, using QEPCAD-B.

$$\left[\begin{array}{l} \gamma \geq 0 \wedge \alpha+\beta+\gamma-\mu-\nu+1 \geq 0 \wedge \\ \left[\beta-\nu+2(\alpha-\mu+1) < 0 \vee \beta-\nu > 0 \vee 4\gamma(\alpha-\mu+1)-(\beta-\nu)^2 \geq 0\right] \end{array}\right] \tag{6}$$

$$\left[\begin{array}{l} \gamma-\nu+1 \geq 0 \wedge \alpha+\beta+\gamma-\mu-\nu+1 \geq 0 \wedge \\ \left[\beta+2\alpha-\mu < 0 \qquad\qquad \vee \beta-\mu > 0 \vee 4\alpha(\gamma-\nu+1)-(\beta-\mu)^2 \geq 0\right] \end{array}\right] \tag{7}$$

Neither Mathematica, nor QEPCAD-B, were able to provide a quantifier-free formula equivalent to the first one in the conjunct above. Redlog outputs, for the same formula, the quantifier-free formula (9). However, we decided, for now, not to use it because it is very long and it is very hard to interpret.

Therefore we proceeded as follows.

Let $C(a,b,\mu,\nu) = 0 < a \leq \frac{\mu a+\nu b}{2} \leq b$, $D(a,b,\mu,\nu,\alpha,\beta,\gamma) = -(\frac{sa+tb}{2})^2 + \alpha a^2 + \beta ab + \gamma b^2 \geq 0$

1. We expressed $C(a,b,\mu,\nu)$ as $C_1(a,b,\mu,nu) \vee \ldots \vee C_k(a,b,\mu,\nu)$, where $C_i(a,b,\mu,\nu) = P_i(\mu,\nu) \wedge Q_i(a,b,\mu,\nu)$. $P_i(\mu,\nu)$ were obtained manually, $Q_i(a,b,\mu,\nu)$ automatically using QEPCAD-B.
2. We proved that:
$$\left[\underset{a,b}{\forall} C(a,b,\mu,\nu) \Rightarrow D(a,b,\mu,\nu,\alpha,\beta,\gamma)\right] \Longleftrightarrow$$
$$\left[\begin{array}{l} \left(P_1(\mu,\nu) \wedge \underset{a,b}{\forall} Q_1(a,b,\mu,\nu)\right) \Rightarrow D(a,b,\mu,\nu,\alpha,\beta,\gamma) \\ \vee \\ \ldots \\ \vee \\ \left(P_k(\mu,\nu) \wedge \underset{a,b}{\forall} Q_k(a,b,\mu,\nu)\right) \Rightarrow D(a,b,\mu,\nu,\alpha,\beta,\gamma) \end{array}\right].$$
3. We carried out quantifier elimination for
$\underset{a,b}{\forall} Q_1(a,b,\mu,\nu) \Rightarrow D(a,b,\mu,\nu,\alpha,\beta,\gamma)$, ... $\underset{a,b}{\forall} Q_k(a,b,\mu,\nu) \Rightarrow D(a,b,\mu,\nu,\alpha,\beta,\gamma)$,
using QEPCAD-B.
4. We combined the formulas obtained at 3. above with $P_1(\mu,\nu)$,..., $P_k(\mu,\nu)$ and simplify the results.

Finally, we obtained:

$$\left[\begin{array}{l} \left[\begin{array}{l} \nu \geq 0 \wedge \mu+\nu > 0 \wedge \mu \geq 0 \wedge \mu-2 \leq 0 \wedge \mu+\nu-2 = 0 \wedge 4\gamma-\mu^2+4\mu-4 \geq 0 \wedge \alpha+\beta+\gamma-1 \geq 0 \wedge \\ \left[\beta+2\alpha-\mu < 0 \vee 2\beta+\mu^2-2\mu > 0 \vee 4\alpha\gamma-\mu^2\gamma-\beta^2-\mu^2\beta+2\mu\beta-\mu^2\alpha+4\mu\alpha-4\alpha \geq 0\right] \end{array}\right] \\ \vee \\ \left[\begin{array}{l} \nu \geq 0 \wedge \mu+\nu > 0 \wedge \mu \geq 0 \wedge \mu-2 \leq 0 \wedge \mu+\nu-2 \leq 0 \wedge 4\gamma-\nu^2 \geq 0 \wedge \\ \mu^2\gamma-4\mu\gamma+4\gamma-\mu\nu\beta+2\nu\beta+\nu^2\alpha-\nu^2 \geq 0 \wedge \\ \left[[\mu-1 \leq 0 \wedge \nu-1 \leq 0] \vee 4\mu-1 \leq 0 \vee 4\nu-1 \leq 0\right] \wedge \\ \left[[2\beta-\mu\nu > 0 \vee \mu\beta-2\beta-2\nu\alpha+\mu\nu > 0 \vee 4\alpha\gamma-\mu^2\gamma-\beta^2+\mu\nu\beta-\nu^2\alpha \geq 0\right] \end{array}\right] \\ \vee \\ \left[\begin{array}{l} \nu \geq 0 \wedge \mu+\nu > 0 \wedge \mu \geq 0 \wedge \mu-2 \leq 0 \wedge \mu+\nu-2 \leq 0 \wedge 4\mu-1 \leq 0 \wedge \gamma \geq 0 \wedge \alpha+\beta+\gamma-1 \geq 0 \wedge \\ \left[\beta+2\alpha-2 < 0 \vee \beta > 0 \vee 4\alpha\gamma-4\gamma-\beta^2 \geq 0\right] \end{array}\right] \end{array}\right] \tag{8}$$

$$
\left[\begin{array}{l}
\left[\ \alpha\nu^2-4\alpha\nu+4\alpha-\beta\mu\nu+2\beta\mu+\gamma\mu^2-\mu^2\geq 0\vee\nu-2=0\vee(\mu\nu-2\mu+\nu^2-4\nu+4\geq 0\wedge\mu+\nu-2\neq 0)\ \right]\\
\wedge\\
\left[\begin{array}{l}
32\alpha\beta\gamma-8\alpha\beta\nu^2-16\alpha\gamma\mu\nu+4\alpha\mu\nu^3-16\beta^3+24\beta^2\mu\nu-8\beta\gamma\mu^2-10\beta\mu^2\nu^2+4\gamma\mu^3\nu+\mu^3\nu^3\geq 0\vee\\
8\alpha\beta\nu-4\alpha\mu\nu^2-8\beta^2\mu+16\beta^2+6\beta\mu^2\nu-16\beta\mu\nu-\mu^3\nu^2+4\mu^2\nu^2\geq 0\vee 2\beta-\mu\nu=0\vee\\
4\gamma-\nu^2\neq 0\vee\left[\begin{array}{l}
8\alpha\beta\nu-16\alpha\beta-4\alpha\mu\nu^2+8\alpha\mu\nu-8\beta^2\mu+6\beta\mu^2\nu+4\beta\mu^2-\mu^3\nu^2-2\mu^3\nu\leq 0\wedge\\
(4\alpha\nu-8\alpha-4\beta\mu+\mu^2\nu+2\mu^2\neq 0\vee\nu-2<0)
\end{array}\right]
\end{array}\right]\\
\wedge\\
\left[\ \nu-2\geq 0\vee(4\gamma-\nu^2\geq 0\wedge(4\gamma-\nu^2>0\vee(2\beta-\mu\nu\geq 0\wedge(4\alpha-\mu^2\geq 0\vee 2\beta-\mu\nu>0))))\ \right]\\
\wedge\\
\left[\begin{array}{l}
4\alpha\gamma-\alpha\nu^2-\beta^2+\beta\mu\nu-\gamma\mu^2>0\vee 4\gamma-\nu^2=0\\
\vee\\
\left[\begin{array}{l}
\left[\begin{array}{l}
4\alpha\gamma-\alpha\nu^2-\beta^2+\beta\mu\nu-\gamma\mu^2<0\vee 4\gamma-\nu^2\geq 0\\
\vee\\
\left[\begin{array}{l}
4\alpha\gamma\nu^2-\alpha\nu^4-4\beta\gamma\mu\nu+8\beta\gamma\nu+\beta\mu\nu^3-2\beta\nu^3+4\gamma^2\mu^2-16\gamma^2\mu+16\gamma^2-\gamma\mu^2\nu^2+4\gamma\mu\nu^2-8\gamma\nu^2+\nu^4\geq 0\wedge\\
4\beta\gamma\nu-\beta\nu^3-8\gamma^2\mu+16\gamma^2+2\gamma\mu\nu^2-8\gamma\nu^2+\nu^4\geq 0
\end{array}\right]\\
\vee\\
\left[\begin{array}{l}
4\alpha\gamma\nu^2-\alpha\nu^4-4\beta\gamma\mu\nu+8\beta\gamma\nu+\beta\mu\nu^3-2\beta\nu^3+4\gamma^2\mu^2-16\gamma^2\mu+16\gamma^2-\gamma\mu^2\nu^2+4\gamma\mu\nu^2-8\gamma\nu^2+\nu^4\leq 0\wedge\\
4\gamma\nu-\nu^3\geq 0
\end{array}\right]\\
\vee\\
\left[\begin{array}{l}
\left[\begin{array}{l}
4\alpha\gamma\nu^2-16\alpha\gamma\nu+16\alpha\gamma-\alpha\nu^4+4\alpha\nu^3-4\alpha\nu^2-4\beta\gamma\mu\nu+8\beta\gamma\mu+\beta\mu\nu^3-2\beta\mu\nu^2+4\gamma^2\mu^2-\\
\quad\gamma\mu^2\nu^2-4\gamma\mu^2+\mu^2\nu^2\leq 0\vee 4\beta\gamma\nu-8\beta\gamma-\beta\nu^3+2\beta\nu^2-8\gamma^2\mu+2\gamma\mu\nu^2+4\gamma\mu\nu-\mu\nu^3\leq 0
\end{array}\right]\\
\wedge\\
\left[\begin{array}{l}
4\gamma\nu-8\gamma-\nu^3+2\nu^2<0\vee\\
\left[\begin{array}{l}
4\alpha\gamma\nu^2-16\alpha\gamma\nu+16\alpha\gamma-\alpha\nu^4+4\alpha\nu^3-4\alpha\nu^2-4\beta\gamma\mu\nu+8\beta\gamma\mu+\beta\mu\nu^3-2\beta\mu\nu^2+4\gamma^2\mu^2-\\
\quad\gamma\mu^2\nu^2-4\gamma\mu^2+\mu^2\nu^2\geq 0\wedge 4\beta\gamma\nu-8\beta\gamma-\beta\nu^3+2\beta\nu^2-8\gamma^2\mu+2\gamma\mu\nu^2+4\gamma\mu\nu-\mu\nu^3\leq 0
\end{array}\right]
\end{array}\right]\\
\wedge\\
\left[\begin{array}{l}
\alpha\nu^2-4\alpha\nu+4\alpha-\beta\mu\nu+2\beta\mu+\gamma\mu^2-\mu^2\neq 0\vee\nu-2<0\vee\\
(\beta\nu^2-4\beta\nu+4\beta-2\gamma\mu\nu+4\gamma\mu+\mu\nu^2-2\mu\nu\geq 0\wedge\beta\nu-2\beta-2\gamma\mu+\mu\nu\neq 0\wedge\nu-2>0)
\end{array}\right]
\end{array}\right]
\end{array}\right]\\
\wedge\\
\left[\begin{array}{l}
\left[\begin{array}{l}
4\alpha\gamma\nu^2-\alpha\nu^4-4\beta\gamma\mu\nu+8\beta\gamma\nu+\beta\mu\nu^3-2\beta\nu^3+4\gamma^2\mu^2-16\gamma^2\mu+16\gamma^2-\gamma\mu^2\nu^2+4\gamma\mu\nu^2-8\gamma\nu^2+\nu^4\geq 0\wedge\\
4\beta\gamma\nu-\beta\nu^3-8\gamma^2\mu+16\gamma^2+2\gamma\mu\nu^2-8\gamma\nu^2+\nu^4\geq 0
\end{array}\right]\\
\vee\\
\left[\begin{array}{l}
4\alpha\gamma\nu^2-\alpha\nu^4-4\beta\gamma\mu\nu+8\beta\gamma\nu+\beta\mu\nu^3-2\beta\nu^3+4\gamma^2\mu^2-16\gamma^2\mu+16\gamma^2-\gamma\mu^2\nu^2+4\gamma\mu\nu^2-8\gamma\nu^2+\nu^4\leq 0\wedge\\
4\gamma\nu-\nu^3\geq 0
\end{array}\right]\\
\vee\\
\left[\ 4\alpha\gamma-\alpha\nu^2-\beta^2+\beta\mu\nu-\gamma\mu^2=0\wedge 4\gamma-\nu^2\geq 0\ \right]\\
\vee\\
\left[\begin{array}{l}
\left[\begin{array}{l}
4\alpha\gamma\nu^2-16\alpha\gamma\nu+16\alpha\gamma-\alpha\nu^4+4\alpha\nu^3-4\alpha\nu^2-4\beta\gamma\mu\nu+8\beta\gamma\mu+\beta\mu\nu^3-2\beta\mu\nu^2+4\gamma^2\mu^2-\gamma\mu^2\nu^2-\\
\quad 4\gamma\mu^2+\mu^2\nu^2\leq 0\vee 4\beta\gamma\nu-8\beta\gamma-\beta\nu^3+2\beta\nu^2-8\gamma^2\mu+2\gamma\mu\nu^2+4\gamma\mu\nu-\mu\nu^3\leq 0
\end{array}\right]\\
\wedge\\
\left[\begin{array}{l}
4\gamma\nu-8\gamma-\nu^3+2\nu^2>0\vee\\
\left[\begin{array}{l}
4\alpha\gamma\nu^2-16\alpha\gamma\nu+16\alpha\gamma-\alpha\nu^4+4\alpha\nu^3-4\alpha\nu^2-4\beta\gamma\mu\nu+8\beta\gamma\mu+\beta\mu\nu^3-2\beta\mu\nu^2+4\gamma^2\mu^2-\gamma\mu^2\nu^2-\\
\quad 4\gamma\mu^2+\mu^2\nu^2\geq 0\wedge 4\beta\gamma\nu-8\beta\gamma-\beta\nu^3+2\beta\nu^2-8\gamma^2\mu+2\gamma\mu\nu^2+4\gamma\mu\nu-\mu\nu^3\leq 0
\end{array}\right]
\end{array}\right]\\
\wedge\\
\left[\begin{array}{l}
\alpha\nu^2-4\alpha\nu+4\alpha-\beta\mu\nu+2\beta\mu+\gamma\mu^2-\mu^2\neq 0\vee\nu-2<0\vee\\
(\beta\nu^2-4\beta\nu+4\beta-2\gamma\mu\nu+4\gamma\mu+\mu\nu^2-2\mu\nu\leq 0\wedge\beta\nu-2\beta-2\gamma\mu+\mu\nu\neq 0\wedge\nu-2>0)
\end{array}\right]
\end{array}\right]
\end{array}\right]
\end{array}\right.
\end{array}\right.
\end{array}\right.
\tag{9}
$$

3.2 Case $\mu < 0 \wedge \nu < 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \leq \sqrt{x} \Longleftrightarrow \\
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \alpha a^2+\beta ab+\gamma b^2+x \leq \sqrt{x}(\mu a+\nu b) \Longleftrightarrow \\
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow x-\sqrt{x}(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2 \leq 0 \Longleftrightarrow \\
\underset{a,b}{\forall}\ 0 < a \leq b \quad \Rightarrow \left[\begin{array}{l} a^2-a(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2 \leq 0 \\ \wedge \\ b^2-b(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2 \leq 0 \end{array}\right] \Longleftrightarrow \\
\left[\begin{array}{l} \underset{a,b}{\forall}\ 0 < a \leq b \quad \Rightarrow a^2-a(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2 \leq 0 \\ \wedge \\ \underset{a,b}{\forall}\ 0 < a \leq b \quad \Rightarrow b^2-b(\mu a+\nu b)+\alpha a^2+\beta ab+\gamma b^2 \leq 0 \end{array}\right].
\end{array}$$

The last formulas are handled by a quantifier elimination software, namely QEPCAD-B. After simplification we obtain:

$$\begin{array}{l}
\gamma \leq 0 \wedge \gamma-\nu+1 \leq 0 \wedge \alpha+\beta+\gamma-\mu-\nu+1 \leq 0 \wedge \\
\big[\beta-\nu < 0 \vee \beta-\nu+2(\alpha-\mu+1) > 0 \vee 4\gamma(\alpha-\mu+1)+(\beta-\nu)^2 \geq 0\big] \wedge \\
\big[\beta-\mu < 0 \vee \beta-2\alpha-\mu > 0 \qquad\qquad \vee 4\alpha(\gamma-\nu+1)+(\beta-\mu)^2 \geq 0\big].
\end{array}$$

3.3 Case $\mu > 0 \wedge \nu < 0 \wedge \mu+\nu = 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
false.
\end{array}$$

3.4 Case $\mu > 0 \wedge \nu < 0 \wedge \mu+\nu > 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
false.
\end{array}$$

3.5 Case $\mu > 0 \wedge \nu < 0 \wedge \mu+\nu < 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
\gamma \leq 0 \wedge \gamma-\nu+1 \leq 0 \wedge \alpha+\beta+\gamma-\mu-\nu+1 \leq 0 \wedge \\
\big[\beta-\nu < 0 \vee \beta-\nu+2(\alpha-\mu+1) > 0 \vee 4\gamma(\alpha-\mu+1)+(\beta-\nu)^2 \geq 0\big] \wedge \\
\big[\beta-\mu < 0 \vee \beta-2\alpha-\mu > 0 \qquad\qquad \vee 4\alpha(\gamma-\nu+1)+(\beta-\mu)^2 \geq 0\big].
\end{array}$$

3.6 Case $\mu < 0 \wedge \nu > 0 \wedge \mu+\nu = 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
false.
\end{array}$$

3.7 Case $\mu < 0 \wedge \nu > 0 \wedge \mu+\nu < 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
false.
\end{array}$$

3.8 Case $\mu < 0 \wedge \nu > 0 \wedge \mu+\nu > 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
(8) \wedge (6) \wedge (7)
\end{array}$$

3.9 Case $\mu > 0 \wedge \nu = 0$.

$$\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \tfrac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow$$
$$(8) \wedge (6) \wedge (7)$$

3.10 Case $\mu = 0 \wedge \nu > 0$.

$$\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \tfrac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow$$
$$(8) \wedge (6) \wedge (7)$$

3.11 Case $\mu = 0 \wedge \nu < 0$.

$$\begin{array}{l}
\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \tfrac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow \\
\gamma \leq 0 \wedge \gamma - \nu + 1 \leq 0 \wedge \alpha + \beta + \gamma - \mu - \nu + 1 \leq 0 \wedge \\
\left[\beta - \nu < 0 \vee \beta - \nu + 2(\alpha - \mu + 1) > 0 \vee 4\gamma(\alpha - \mu + 1) + (\beta - \nu)^2 \geq 0\right] \wedge \\
\left[\beta - \mu < 0 \vee \beta - 2\alpha - \mu > 0 \qquad\qquad \vee 4\alpha(\gamma - \nu + 1) + (\beta - \mu)^2 \geq 0\right].
\end{array}$$

3.12 Case $\mu < 0 \wedge \nu = 0$. $\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow \tfrac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \geq \sqrt{x} \Longleftrightarrow$

$$\begin{array}{l}
\gamma \leq 0 \wedge \gamma - \nu + 1 \leq 0 \wedge \alpha + \beta + \gamma - \mu - \nu + 1 \leq 0 \wedge \\
\left[\beta - \nu < 0 \vee \beta - \nu + 2(\alpha - \mu + 1) > 0 \vee 4\gamma(\alpha - \mu + 1) + (\beta - \nu)^2 \geq 0\right] \wedge \\
\left[\beta - \mu < 0 \vee \beta - 2\alpha - \mu > 0 \vee 4\alpha(\gamma - \nu + 1) + (\beta - \mu)^2 \geq 0\right].
\end{array}$$

□

Combining the three lemmas, we obtain the following theorem:

Theorem 3. $\underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow 0 < \tfrac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \leq \tfrac{\alpha a^2+\beta ab+\gamma b^2+x}{\mu a+\nu b} \Longleftrightarrow$

$$\left[\begin{array}{l}
\left[\begin{array}{l}
r = 0 \wedge q \geq 0 \wedge t - 1 \geq 0 \wedge t - q \geq 0 \wedge s + t > 0 \wedge p + q + 1 > 0 \wedge t + s - p - q - 1 \geq 0 \wedge \\
\left[s - q > 0 \vee s - q - 2p < 0 \vee 4p(t-1) + (s-q)^2 \leq 0\right]
\end{array}\right] \\
\bigwedge \\
\left[\begin{array}{l}
\left[\begin{array}{l}
\left[\begin{array}{l}
\left[\begin{array}{l}
\nu \geq 0 \wedge \mu + \nu > 0 \wedge \mu \geq 0 \wedge \mu - 2 \leq 0 \wedge \mu + \nu - 2 = 0 \wedge 4\gamma - \mu^2 + 4\mu - 4 \geq 0 \wedge \alpha + \beta + \gamma - 1 \geq 0 \wedge \\
\left[\beta + 2\alpha - \mu < 0 \vee 2\beta + \mu^2 - 2\mu > 0 \vee 4\alpha\gamma - \mu^2\gamma - \beta^2 - \mu^2\beta + 2\mu\beta - \mu^2\alpha + 4\mu\alpha - 4\alpha \geq 0\right]
\end{array}\right. \\
\vee \\
\left[\begin{array}{l}
\nu \geq 0 \wedge \mu + \nu > 0 \wedge \mu \geq 0 \wedge \mu - 2 \leq 0 \wedge \mu + \nu - 2 \leq 0 \wedge 4\gamma - \nu^2 \geq 0 \wedge \\
\mu^2\gamma - 4\mu\gamma + 4\gamma - \mu\nu\beta + 2\nu\beta + \nu^2\alpha - \nu^2 \geq 0 \wedge \\
\left[[\mu - 1 \leq 0 \wedge \nu - 1 \leq 0] \vee 4\mu - 1 \leq 0 \vee 4\nu - 1 \leq 0\right] \wedge \\
\left[[2\beta - \mu\nu > 0 \vee \mu\beta - 2\beta - 2\nu\alpha + \mu\nu > 0 \vee 4\alpha\gamma - \mu^2\gamma - \beta^2 + \mu\nu\beta - \nu^2\alpha \geq 0\right]
\end{array}\right. \\
\vee \\
\left[\begin{array}{l}
\nu \geq 0 \wedge \mu + \nu > 0 \wedge \mu \geq 0 \wedge \mu - 2 \leq 0 \wedge \mu + \nu - 2 \leq 0 \wedge 4\mu - 1 \leq 0 \wedge \gamma \geq 0 \wedge \alpha + \beta + \gamma - 1 \geq 0 \wedge \\
\left[\beta + 2\alpha - 2 < 0 \vee \beta > 0 \vee 4\alpha\gamma - 4\gamma - \beta^2 \geq 0\right]
\end{array}\right.
\end{array}\right. \\
\wedge \\
\gamma \geq 0 \wedge \alpha + \beta + \gamma - \mu - \nu + 1 \geq 0 \wedge \left[\beta - \nu + 2(\alpha - \mu + 1) < 0 \vee \beta - \nu > 0 \vee 4\gamma(\alpha - \mu + 1) - (\beta - \nu)^2 \geq 0\right] \\
\wedge \\
\gamma - \nu + 1 \geq 0 \wedge \left[\beta + 2\alpha - \mu < 0 \vee \beta - \mu > 0 \vee 4\alpha(\gamma - \nu + 1) - (\beta - \mu)^2 \geq 0\right]
\end{array}\right. \\
\bigvee \\
\left[\begin{array}{l}
\nu \leq 0 \wedge \mu + \nu < 0 \wedge \gamma \leq 0 \wedge \gamma - \nu + 1 \leq 0 \wedge \alpha + \beta + \gamma - \mu - \nu + 1 \leq 0 \wedge \\
\left[\beta - \nu < 0 \vee \beta - \nu + 2(\alpha - \mu + 1) > 0 \vee 4\gamma(\alpha - \mu + 1) + (\beta - \nu)^2 \geq 0\right] \wedge \\
\left[\beta - \mu < 0 \vee \beta - 2\alpha - \mu > 0 \qquad\qquad \vee 4\alpha(\gamma - \nu + 1) + (\beta - \mu)^2 \geq 0\right]
\end{array}\right.
\end{array}\right.
\end{array}\right.$$

4 Conclusion and Future Work

We have presented two challenging problems (algorithm correctness and optimization) that were approached using powerful polynomial algebra (resultant and Bézoutian computation, cylindrical algebraic decomposition) and numerical (interpolation) methods.

Immediate goal of this research is to find the parameters of the loop assignments such that *Algorithm 3* is optimal, given the necessary and sufficient conditions presented in this paper. Also, we plan to automatize parts of the parameters synthesis, namely those parts which could not be handled by state-of-the-art quantifier elimination software. Regarding the method presented in *Section 2*, we plan to extend it to multivariate polynomials and multiple loop assignments.

Acknoledgements

This work has been performed during the author's visit to Department of Mathematics, North Carolina State University, Raleigh, USA, supported by a fellowship of Austrian Marshall Plan Foundation.

I express special thanks to Prof. Hoon Hong from the North Carolina State University for suggesting the directions of research presented in this paper, for his contagious research enthusiasm and for introducing me to American hospitality.

I am grateful to my PhD advisor, Prof. Tudor Jebelean, for presenting me fellowship opportunity and for his continuous encouragements and support.

References

[1] C. Brown, *QEPCAD-B: a program for computing with Semi-Algebraic sets using CADs*, SIGSAM Bull. **37** (2003), no. 4, 97–108.

[2] A. Bundy, L. Dixon, J. Gow, and J. Fleuriot, *Constructing induction rules for deductive synthesis proofs*, Electron. Notes Theor. Comput. Sci. **153** (2006), 3–21.

[3] G. Collins and H. Hong, *Partial cylindrical algebraic decomposition for quantifier elimination*, J. Symb. Comput. **12** (1991), no. 3, 299–328.

[4] G. E. Collins, *Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition*, LNCS **33** (1975), 134–183.

[5] D. Cox, J. Little, and D. O'Shea, *Ideal, varieties, and algorithms. an introduction to computational algebraic geometry and commutative algebra*, second ed., Springer, 1998.

[6] J. Davenport and J. Heintz, *Real quantifier elimination is doubly exponential*, J. Symb. Comput. **5** (1988), no. 1-2, 29–35.

[7] L. de Moura and N. Björner, *Z3: An efficient SMT solver*, TACAS, 2008, pp. 337–340.

[8] A. Dolzmann and T. Sturm, *REDLOG: computer algebra meets computer logic*, SIGSAM Bull. **31** (1997), 2–9.

[9] M. Eraşcu and T. Jebelean, *A calculus for imperative programs: Formalization and implementation*, Proc. of SYNASC 2009 (S. Watt, V. Negru, T. Ida, T. Jebelean, D. Petcu, and D. Zaharie, eds.), IEEE, 2009, p. 77–84.

[10] J. Harrison, *Verifying nonlinear real formulas via sums of squares*, Proc of TPHOLs 2007 (Kaiserslautern, Germany) (K. Schneider and J. Brandt, eds.), LNCS, vol. 4732, Springer-Verlag, 2007, p. 102–118.

[11] H. Hong, *An improvement of the projection operator in cylindrical algebraic decomposition*, Proc. of ISSAC 1990 (New York, NY, USA), ACM, 1990, p. 261–264.

[12] D. Kapur, *Automatically generating loop invariants using quantifier elimination*, Proc. of ACA 2004, 2004.

[13] L. Kovacs, *Automated invariant generation by algebraic techniques for imperative program verification in Theorema*, Ph.D. thesis, RISC, Johannes Kepler University Linz, Austria, October 2007, RISC Technical Report No. 07-16.

[14] P. Lancaster and M. Tismenetsky, *The theory of matrices: with applications*, Computer science and applied mathematics, Academic Press, 1985.

[15] A. Marco and J. J. Martinez, *Implicitization of rational surfaces by means of polynomial interpolation*, Computer Aided Geometric Design **19** (2002), no. 5, 327 – 344.

[16] M. Minimair, *Resultants of composed polynomials*, Ph.D. thesis, North Carolina State University, 2001.

[17] A. Platzer and J. Quesel, *KeYmaera: a hybrid theorem prover for hybrid systems*, Proc. of IJCAR 2008, Sydney, Australia (A. Armando, P. Baumgartner, and G. Dowek, eds.), LNCS, vol. 5195, Springer, 2008, pp. 171–178.

[18] A. Platzer, J. Quesel, and P. Rümmer, *Real world verification*, Automated Deduction – CADE-22 (Berlin, Heidelberg) (Renate Schmidt, ed.), Lecture Notes in Computer Science, vol. 5663, Springer Berlin / Heidelberg, 2009, pp. 485–501.

[19] E. Rodriguez-Carbonell and D. Kapur, *Automatic generation of polynomial loop invariants: Algebraic foundations*, Proc. of ISSAC 2004 (Santander, Spain), 2004.

[20] S. Sankaranaryanan, B. S. Henry, and Z. Manna, *Non-linear loop invariant generation using Gröbner bases*, Proc. of POPL 2004 (Venice, Italy), 2004.

[21] V. Weispfenning, *The complexity of linear problems in fields*, J. Symb. Comput. **5** (1988), 3–27.

[22] S. Wolfram, *The Mathematica book. version 5.0*, Wolfram Media, 2003.

A Additional Proofs

A.1 Additional Proofs Lemma 1

Lemma 4. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s>0 \wedge t>0 \Longrightarrow \left[\begin{array}{ll} \underset{a,b,x}{\forall}\ 0<a\leq\sqrt{x}\leq b \Rightarrow pa^2+qab+rb^2+x>0 \Longleftrightarrow & \\ \underset{a,b}{\forall}\ 0<a\leq b \qquad\qquad \Rightarrow (p+1)a^2+qab+rb^2>0 & \end{array}\right].$$

Proof. Take p_0,q_0,r_0,s_0,t_0 arbitrary. Assume $s_0>0\wedge t_0>0$. Prove

$$\left[\begin{array}{ll} \underset{a,b,x}{\forall}\ 0<a\leq\sqrt{x}\leq b \Rightarrow p_0a^2+q_0ab+r_0b^2+x>0 \Longleftrightarrow & \\ \underset{a,b}{\forall}\ 0<a\leq b \qquad\qquad \Rightarrow (p_0+1)a^2+q_0ab+r_0b^2>0 & \end{array}\right].$$

We prove each direction.

” $\Longrightarrow$ ”. Take a_0,b_0 arbitrary. Assume $0<a_0\leq b_0$. Prove $(p_0+1)a_0^2+q_0a_0b_0+r_0b0^2>0$.

Instantiate in assumptions $a=a_0$, $b=b_0$, $x=a_0^2$, obtaining:

$0<a_0\leq\sqrt{a_0^2}\leq b_0\Rightarrow p_0a_0^2+q_0a_0b_0+r_0b_0^2+a_0^2>0.$

Since $0<a_0\leq a_0\leq b_0$ is true, $p_0a_0^2+q_0a_0b_0+r_0b_0^2+a_0^2>0$ is true, which is equivalent to the goal.

” $\Longleftarrow$ ”. Take a_0,b_0,x_0 arbitrary. Assume $0<a_0\leq\sqrt{x_0}\leq b_0$. Prove $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0>0$. Instantiate in assumptions $a=a_0$, $b=b_0$, obtaining:

$0<a_0\leq b_0\Rightarrow(p_0+1)a_0^2+q_0a_0b_0+r_0b_0^2>0.$

Since $0<a_0\leq b_0$ is true, $(p_0+1)a_0^2+q_0a_0b_0+r_0b_0^2>0=p_0a_0^2+q_0a_0b_0+r_0b_0^2+a_0^2>0$ is true.

But $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x=\underbrace{p_0a_0^2+q_0a_0b_0+r_0b_0^2+a_0^2}_{>0}+\underbrace{x_0-a_0^2}_{\geq0}>0$. Thus the goal is proved.

□

Lemma 5. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s<0\wedge t<0 \Longrightarrow \left[\begin{array}{ll} \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow pa^2+qab+rb^2+x<0 \Longleftrightarrow & \\ \underset{a,b}{\forall}\ 0<a\le b \qquad\qquad \Rightarrow (r+1)b^2+qab+pa^2<0 & \end{array}\right].$$

Proof. Take p_0,q_0,r_0,s_0,t_0 arbitrary. Assume $s_0<0\wedge t_0<0$. Prove

$$\left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow pa^2+qab+rb^2+x<0 \Longleftrightarrow \\ \underset{a,b}{\forall}\ 0<a\le b \qquad\qquad \Rightarrow (r+1)b^2+qab+pa^2<0 \end{array}\right].$$

We prove each direction.

" $\Longrightarrow$ ". Take a_0,b_0 arbitrary. Assume $0<a_0\le b_0$. Prove $(r_0+1)b_0^2+q_0a_0b_0+p_0a_0^2<0$. Instantiate in assumptions $a=a_0$, $b=b_0$, $x=b_0^2$, obtaining:

$0<a_0\le\sqrt{b_0^2}\le b_0 \Rightarrow p_0a_0^2+q_0a_0b_0+r_0b_0^2+b_0^2<0.$

Since $0<a_0\le b_0\le b_0$ is true, $p_0a_0^2+q_0a_0b_0+r_0b_0^2+b_0^2(r_0+1)b_0^2+q_0a_0b_0+p_0a_0^2<0$ is true, which is equivalent to the goal.

" $\Longleftarrow$ ". Take a_0,b_0,x_0 arbitrary. Assume $0<a_0\le\sqrt{x_0}\le b_0$. Prove $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0<0$. Instantiate in assumptions $a=a_0$, $b=b_0$, obtaining:

$0<a_0\le b_0 \Rightarrow p_0a_0^2+q_0a_0b_0+r_0b_0^2+b_0^2<0.$

Since $0<a_0\le b_0$ is true, $p_0a_0^2+q_0a_0b_0+r_0b_0^2+b_0^2<0$ is true.

But $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x=\underbrace{p_0a_0^2+q_0a_0b_0+r_0b_0^2+b_0^2}_{<0}+\underbrace{x_0-b_0^2}_{\le 0}<0$. Thus the goal is proved.

□

Lemma 6. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s>0\wedge t<0\wedge s+t=0 \Longrightarrow \left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb)>0 \Longleftrightarrow \\ false \end{array}\right].$$

Proof. Take p_0,q_0,r_0,s_0,t_0 arbitrary. Assume $s_0>0\wedge t_0<0\wedge s_0+t_0=0$. Prove

$$\left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow (p_0a^2+q_0ab+r_0b^2+x)(s_0a+t_0b)>0 \Longleftrightarrow \\ false \end{array}\right].$$

We prove each direction.

" $\Longrightarrow$ ". We prove the contrapositive, i. e.

$\underset{a,b,x}{\exists}\ 0<a\le\sqrt{x}\le b\wedge(p_0a^2+q_0ab+r_0b^2+x)(s_0a+t_0b)\le 0.$

Take $a=b=x=1$. We obtain $0<1\le\sqrt{1}\le 1\wedge(p_0+q_0+r_0+1)(s_0+t_0)=0\le 0$. Thus the goal is proved.

" $\Longleftarrow$ ". Evidently true.

□

Lemma 7. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s>0\wedge t<0\wedge s+t<0 \Longrightarrow \left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow (pa^2+qab+rb^2+x)(sa+tb)>0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow pa^2+qab+rb^2+x<0 \end{array}\right].$$

Proof. Take p_0,q_0,r_0,s_0,t_0 arbitrary. Assume $s_0>0\wedge t_0<0\wedge s_0+t_0<0$. Prove

$$\left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow (p_0a^2+q_0ab+r_0b^2+x)(s_0a+t_0b)>0 \Longleftrightarrow \\ \underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow p_0a^2+q_0ab+r_0b^2+x<0 \end{array}\right].$$

We prove each direction.

" $\Longrightarrow$ ". Take a_0, b_0, x_0 arbitrary. Assume $0<a_0\le\sqrt{x_0}\le b_0$. Prove $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0<0$.

Instantiate in assumption $a=a_0$, $b=b_0$, $x=x_0$, obtaining:

$0 < a_0 \le \sqrt{x_0} \le b_0 \Rightarrow (p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0)(s_0a_0+t_0b_0) > 0.$

Because $0 < a_0 \le \sqrt{x_0} \le b_0$ is true, $(p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0)(s_0a_0+t_0b_0) > 0$ is true.

But $s_0a_0+t_0b_0 = \underbrace{(s_0+t_0)}_{<0}\underbrace{a_0}_{>0}+\underbrace{b_0-a_0}_{\ge 0}\underbrace{t_0}_{<0} < 0$. Therefore $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0 < 0$, which is actually the goal.

"$\Longleftarrow$". Take a_0, b_0, x_0 arbitrary. Assume $0 < a_0 \le \sqrt{x_0} \le b_0$. Prove $(p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0)(s_0a_0+t_0b_0) > 0$.

Instantiate in assumption $a = a_0$, $b = b_0$, $x = x_0$, obtaining:

$0 < a_0 \le \sqrt{x_0} \le b_0 \Rightarrow p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0 < 0.$

Because $0 < a_0 \le \sqrt{x_0} \le b_0$ is true, $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0 < 0$ is true.

But $s_0a_0+t_0b_0 < 0$. Therefore $(p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0)(s_0a_0+t_0b_0) > 0$, which is actually the goal.

□

A.2 Additional Proofs Lemma 2

Lemma 8. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s > 0 \wedge t > 0 \Longrightarrow \left[\begin{array}{lll} \underset{a,b,x}{\forall} 0 < a \le \sqrt{x} \le b \Rightarrow x - \sqrt{x}(sa+tb)+pa^2+qab+rb^2+x \le 0 \Longleftrightarrow & & \\ \underset{a,b}{\forall}\ 0 < a \le b & \Rightarrow & \left[\begin{array}{l} a^2 - a(sa+tb)+pa^2+qab+rb^2 \le 0 \\ \wedge \\ b^2 - b(sa+tb)+pa^2+qab+rb^2 \le 0 \end{array}\right] \end{array}\right]$$

Proof. Take p_0,q_0,r_0,s_0,t_0 arbitrary. Assume $s_0 > 0$, $t_0 > 0$. Prove

$$\left[\begin{array}{lll} \underset{a,b,x}{\forall} 0 < a \le \sqrt{x} \le b \Rightarrow x - \sqrt{x}(s_0a+t_0b)+p_0a^2+q_0ab+r_0b^2+x \le 0 \Longleftrightarrow & & \\ \underset{a,b}{\forall}\ 0 < a \le b & \Rightarrow & \left[\begin{array}{l} a^2 - a(s_0a+t_0b)+p_0a^2+q_0ab+r_0b^2 \le 0 \\ \wedge \\ b^2 - b(s_0a+t_0b)+p_0a^2+q_0ab+r_0b^2 \le 0 \end{array}\right] \end{array}\right].$$

We prove each direction.

"$\Longrightarrow$". Take a_0,b_0 arbitrary. Assume $0 < a_0 \le b_0$. Prove $a_0^2 - a_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$ and $b_0^2 - b_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$.

Instantiate in assumption: $a = a_0$, $b = b_0$, $x = a_0^2$, $x = a_0^2$, obtaining:

$0 < a_0 \le \sqrt{a_0^2} \le b \Rightarrow a_0^2 - a_0(s_0a+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$ and

$0 < a_0 \le \sqrt{b_0^2} \le b \Rightarrow b_0^2 - b_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0.$

Because $0 < a_0 \le \sqrt{a_0^2} \le b$ and $0 < a_0 \le \sqrt{b_0^2} \le b$ are true, $a_0^2 - a_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$ and $b_0^2 - b_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$ are true, which are actually the goal.

"$\Longleftarrow$". Take a_0,b_0,x_0 arbitrary. Assume $0 < a_0 \le \sqrt{x_0} \le b_0$. Prove $x_0 - \sqrt{x_0}(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$.

Instantiate in assumption: $a = a_0$, $b = b_0$, obtaining:

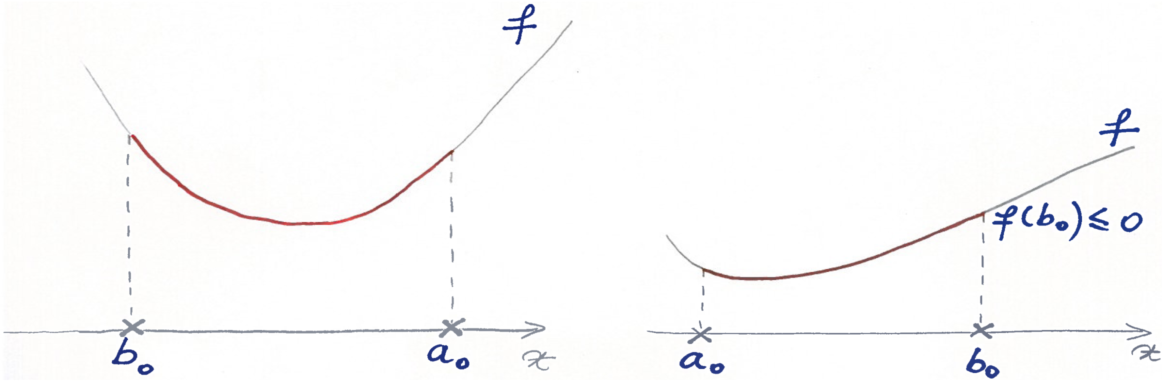
$$0 < a_0 \le b_0 \Rightarrow \left[\begin{array}{l} a_0^2 - a_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0 \\ \wedge \\ b_0^2 - b_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0 \end{array}\right].$$

Because $0 < a_0 \le b_0$ is true, $a_0^2 - a_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$ and $b_0^2 - b_0(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2 \le 0$ are true.

Let $f(\sqrt{x_0}) = x_0 - \sqrt{x_0}(s_0a_0+t_0b_0)+p_0a_0^2+q_0a_0b_0+r_0b_0^2$. f is convex.

Consider the cases in *Figure A.2*.

Figure 1: Shape of $f(\sqrt{x_0}) = x_0 - \sqrt{x}(s_0a_0 + t_0b_0) + p_0a_0^2 + q_0a_0b_0 + r_0b_0^2$ on $[a_0, b_0]$ (*Lemma 8*).



1. Prove $b_0 < a_0 \Rightarrow [0 < a_0 \leq b_0 \Rightarrow f(\sqrt{x}) \leq 0]$.

   But $\left[b_0 < a_0 \Rightarrow [0 < a_0 \leq b_0 \Rightarrow f(\sqrt{x}) \leq 0]\right] \Longleftrightarrow \left[b_0 < a_0 \wedge 0 < a_0 \leq b_0 \Rightarrow f(\sqrt{x}) \leq 0\right] \Longleftrightarrow \left[false \Rightarrow f(\sqrt{x}) \leq 0\right] \Longleftrightarrow true$.

2. Prove $0 < a_0 \leq b_0 \Rightarrow f(\sqrt{x}) \leq 0$.

   Let $f(a_0)$ and $f(b_0)$ be two values of the function. Assume w.l.o.g. that $f(b_0)$ is the maximum of the function.

   But $f(b_0) = b_0^2 - b_0(s_0a_0 + t_0b_0) + p_0a_0^2 + q_0a_0b_0 + r_0b_0^2 \leq 0$. Therefore $f(\sqrt{x_0}) \leq 0$, for $0 < a_0 \leq \sqrt{x_0} \leq b_0$.

□

Lemma 9. *Prove that:*

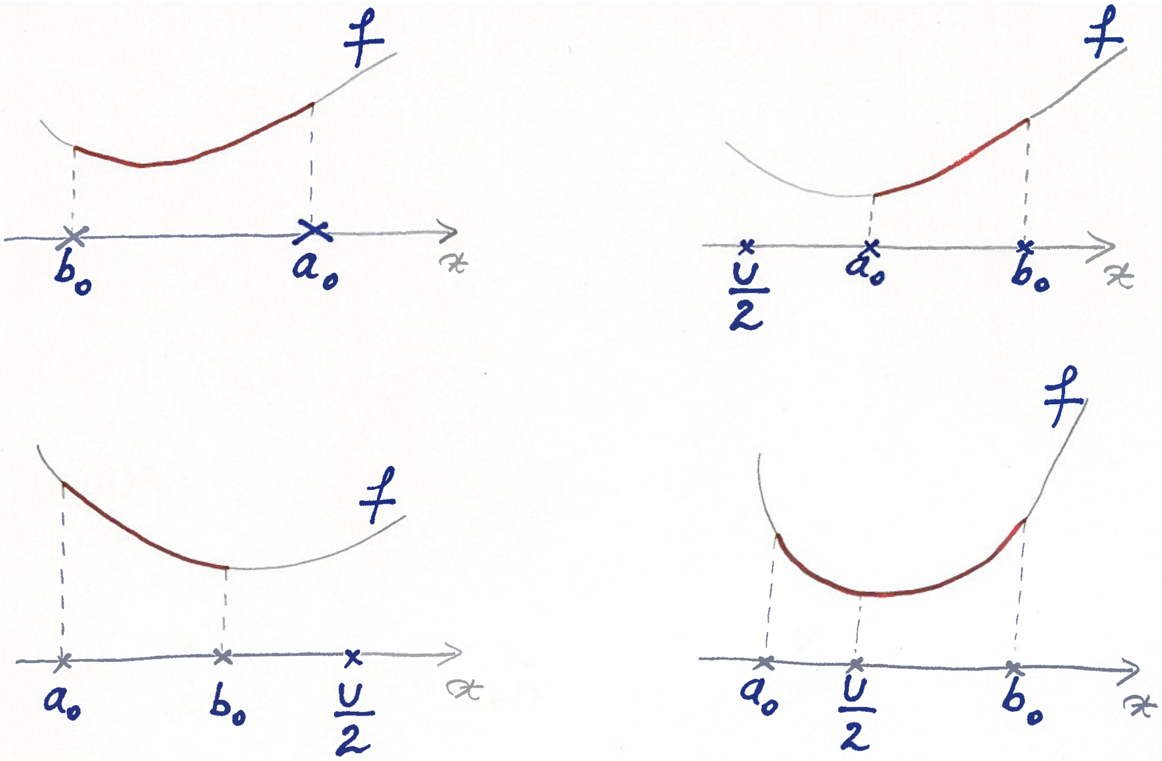
$$\underset{p,q,r,s,t}{\forall} s < 0 \wedge t < 0 \Longrightarrow \left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow x - \sqrt{x}(sa+tb) + pa^2 + qab + rb^2 \geq 0 \Longleftrightarrow \\ \left[\begin{array}{ll} \underset{a,b}{\forall} a \leq \frac{sa+tb}{2} \leq b \Rightarrow [0 < a \leq b \Rightarrow -(\frac{sa+tb}{2})^2 + pa^2 + qab + rb^2 \geq 0 & \\ \wedge & \\ \underset{a,b}{\forall} & 0 < a \leq b \Rightarrow a^2 - a(sa+tb) + pa^2 + qab + rb^2 \geq 0 \\ \wedge & \\ \underset{a,b}{\forall} & 0 < a \leq b \Rightarrow b^2 - b(sa+tb) + pa^2 + qab + rb^2 \geq 0 \end{array}\right] \end{array}\right]$$

Proof. Take p_0, q_0, r_0, s_0, t_0 arbitrary. Prove

$$\left[\begin{array}{l} \underset{a,b,x}{\forall}\ 0 < a \leq \sqrt{x} \leq b \Rightarrow x - \sqrt{x}(s_0a+t_0b) + p_0a^2 + q_0ab + r_0b^2 \geq 0 \Longleftrightarrow \\ \left[\begin{array}{ll} \underset{a,b}{\forall} a \leq \frac{s_0a+t_0b}{2} \leq b \Rightarrow [0 < a \leq b \Rightarrow -(\frac{s_0a+t_0b}{2})^2 + p_0a^2 + q_0ab + r_0b^2 \geq 0] & \\ \wedge & \\ \underset{a,b}{\forall} & 0 < a \leq b \Rightarrow a^2 - a(s_0a+t_0b) + p_0a^2 + q_0ab + r_0b^2 \geq 0 \\ \wedge & \\ \underset{a,b}{\forall} & 0 < a \leq b \Rightarrow b^2 - b(s_0a+t_0b) + p_0a^2 + q_0ab + r_0b^2 \geq 0 \end{array}\right]. \end{array}\right].$$

Denote $U = s_0a + t_0b$ and $V = p_0a_0^2 + q_0a_0b_0 + r_0b_0^2$.
Take $f(\sqrt{x}) = x - U\sqrt{x} + V$.
The goal can be rewritten as:

Figure 2: Shape of $f(\sqrt{x}) = x - U\sqrt{x} + V$ on $[a_0, b_0]$ (*Lemma 9*).



$$\left[\begin{array}{l}\left[\underset{a,b,x}{\forall}\ 0<a\le\sqrt{x}\le b \Rightarrow f(\sqrt{x})\ge 0\right] \iff \\ \left[\left[\underset{a,b}{\forall} 0<a\le \frac{U}{2}\le b\Rightarrow f(\frac{U}{2})\ge 0\right]\wedge \left[\underset{a,b}{\forall} 0<a\le b\Rightarrow f(a)\ge 0\right]\wedge\left[\underset{a,b}{\forall} 0<a\le b\Rightarrow f(b)\ge 0\right]\right]\end{array}\right].$$

We prove each direction.

” $\Longrightarrow$ ”. We prove each conjunct individually.

1. Take a_0, b_0 arbitrary. Assume $0 < a_0 \le \frac{U}{2} \le b_0$. Prove $f(\frac{U}{2}) \ge 0$.

   Instantiate in assumption $a = a_0$, $b = b_0$, $x = (\frac{U}{2})^2$, obtaining: $0 < a_0 \le \sqrt{(\frac{U}{2})^2} \le b_0 \Rightarrow f(\frac{U}{2}) \ge 0$. Because $0 < a_0 \le \frac{U}{2} \le b_0$ is true, $f(\frac{U}{2}) \ge 0$ is true, which is actually the goal.

2. Take a_0, b_0 arbitrary. Assume $0 < a_0 \le b_0$. Prove $f(a_0) \ge 0$.

   Instantiate in assumption $a = a_0$, $b = b_0$, $x = a_0^2$, obtaining: $a_0 \le \sqrt{a_0^2} \le b_0 \Rightarrow f(\sqrt{a_0^2}) \ge 0$. Because $0 < a_0 \le a_0 \le b_0$ is true, $f(a_0) \ge 0$ is true, which is actually the goal.

3. Take a_0, b_0 arbitrary. Assume $0 < a_0 \le b_0$. Prove $f(b_0) \ge 0$.

   Instantiate in assumption $a = a_0$, $b = b_0$, $x = b_0^2$, obtaining: $a_0 \le \sqrt{b_0^2} \le b_0 \Rightarrow f(\sqrt{b_0^2}) \ge 0$. Because $a_0 \le b_0 \le b_0$ is true, $f(b_0) \ge 0$ is true, which is actually the goal.

” $\Longleftarrow$ ”. Take a_0, b_0, x_0 arbitrary. Assume $a_0 \le \sqrt{x_0} \le b_0$. Prove $f(\sqrt{x_0}) \ge 0$.
Instantiate in assumptions $a = a_0$, $b = b_0$, obtaining:
$0 < a_0 \le \sqrt{x_0} \le b_0 \Rightarrow f(\frac{U}{2}) \ge 0$, $0 < a_0 \le b_0 \Rightarrow f(a_0) \ge 0$ and $0 < a_0 \le b_0 \Rightarrow f(b_0) \ge 0$.
Consider the cases in *Figure A.2*.

1. Case $b_0 < a_0$. We have to prove that: $b_0 < a_0 \Rightarrow [0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow f(\sqrt{x_0}) \geq 0]$.

   But $\left[b_0 < a_0 \Rightarrow [0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow f(\sqrt{x_0}) \geq 0]\right] \Longleftrightarrow$
   $\left[b_0 < a_0 \wedge 0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow f(\sqrt{x_0}) \geq 0\right] \Longleftrightarrow \left[false \Rightarrow f(\sqrt{x_0}) \geq 0\right] \Longleftrightarrow true.$

2. Case $\frac{U}{2} < a_0 \leq b_0$. We have to prove that: $\frac{U}{2} < a_0 \leq b_0 \Rightarrow [0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow f(\sqrt{x_0}) \geq 0]$.

   But f is monotonic on $[a_0, b_0]$, $f(a_0) \geq 0$ and $f(b_0) \geq 0$. Therefore $f(\sqrt{x_0}) \geq 0$ on $[a_0, b_0]$.

3. Case $a_0 \leq b_0 < \frac{U}{2}$. We have to prove that: $a_0 \leq b_0 < \frac{U}{2} \Rightarrow [0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow f(\sqrt{x_0}) \geq 0]$.

   But f is monotonic on $[a_0, b_0]$, $f(a_0) \geq 0$ and $f(b_0) \geq 0$. Therefore $f(\sqrt{x_0}) \geq 0$ on $[a_0, b_0]$.

4. Case $a_0 \leq \frac{U}{2} \leq b_0$. We have to prove that: $a_0 \leq \frac{U}{2} \leq b_0 \Rightarrow [0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow f(\sqrt{x_0}) \geq 0]$.

   But f is convex and $f\prime(\sqrt{x_0}) = \frac{U}{2}$. Therefore $\frac{U}{2}$ is a minimum and further $f(\frac{U}{2}) \geq 0$. We conclude that $f(\sqrt{x_0}) \geq 0$ on $[a_0, b_0]$.

□

Lemma 10. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s < 0 \wedge t < 0 \Longrightarrow \left[\begin{array}{l} \underset{a,b}{\forall} 0 < a \leq \frac{sa+tb}{2} \leq b \Rightarrow -(\frac{sa+tb}{2})^2 + pa^2 + qab + rb^2 \geq 0 \Longleftrightarrow \\ true \end{array}\right]$$

Proof. Take p_0, q_0, r_0, s_0, t_0 arbitrary. Assume $s_0 < 0$ and $t_0 < 0$.

Prove $\underset{a,b}{\forall} 0 < a \leq \frac{s_0a+t_0b}{2} \leq b \Rightarrow -(\frac{s_0a+t_0b}{2})^2 + p_0a^2 + q_0ab + r_0b^2 \geq 0 \Longleftrightarrow true.$

But $true \Longleftrightarrow \left[\underset{a,b}{\forall} 0 < a \leq \frac{s_0a+t_0b}{2} \leq b \Rightarrow -(\frac{s_0a+t_0b}{2})^2 + p_0a^2 + q_0ab + r_0b^2 \geq 0\right] \overset{s_0<0 \wedge t_0<0 \wedge a>0 \wedge b>0 \Rightarrow s_0a+t_0b<0}{\Longleftrightarrow}$
$\left[false \Rightarrow -(\frac{s_0a+t_0b}{2})^2 + p_0a^2 + q_0ab + r_0b^2 \geq 0\right] \Longleftrightarrow true.$ □

Lemma 11. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s > 0 \wedge t < 0 \wedge s+t = 0 \Longrightarrow \left[\begin{array}{l} \underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \Rightarrow \frac{pa^2+qab+rb^2+x}{sa+tb} \leq \sqrt{x} \Longleftrightarrow \\ \left[\begin{array}{l} \underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \wedge sa+tb < 0 \Rightarrow pa^2+qab+rb^2+x \geq \sqrt{x}(sa+tb) \\ \wedge \\ \underset{a,b,x}{\forall} \neg(0 < a \leq \sqrt{x} \leq b \wedge sa+tb = 0) \end{array}\right] \end{array}\right].$$

Proof. Take p_0, q_0, r_0, s_0, t_0 arbitrary. Assume $s_0 > 0$, $t_0 < 0$, $s_0 + t_0 = 0$. Prove

$$\left[\begin{array}{l} \underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \wedge s_0a+t_0b < 0 \Rightarrow p_0a^2+q_0ab+r_0b^2+x \geq \sqrt{x}(s_0a+t_0b) \\ \wedge \\ \underset{a,b,x}{\forall} \neg(0 < a \leq \sqrt{x} \leq b \wedge s_0a+t_0b = 0) \end{array}\right].$$

" $\Longrightarrow$ ". We prove each conjunct individually.

1. Proof of $\underset{a,b,x}{\forall} 0 < a \leq \sqrt{x} \leq b \wedge s_0a + t_0b < 0 \Rightarrow p_0a^2 + q_0ab + r_0b^2 + x \geq \sqrt{x}(s_0a + t_0b)$.

   Take a_0, b_0, x_0 arbitrary. Assume $0 < a_0 \leq \sqrt{x} \leq b_0$, $s_0a_0 + t_0b_0 < 0$. Prove $p_0a_0^2 + q_0a_0b_0 + r_0b_0^2 + x \geq \sqrt{x_0}(s_0a_0 + t_0b_0)$.

   Instantiate in assumption $a = a_0, b = b_0, x = x_0$, obtaining $0 < a_0 \leq \sqrt{x_0} \leq b_0 \Rightarrow \frac{p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0}{s_0a_0+t_0b_0} \leq \sqrt{x}$.

   Because $0 < a_0 \leq \sqrt{x_0} \leq b_0$ is true, $\frac{p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0}{s_0a_0+t_0b_0} \leq \sqrt{x}$ is true.

But $s_0a_0+t_0b_0 = \underbrace{(s_0+t_0)}_{=0}\underbrace{a_0}_{>0}+\underbrace{t_0}_{<0}\underbrace{(b_0-a_0)}_{\geq 0} \leq 0$.

Because $s_0a_0+t_0b_0 \leq 0$ is true, $p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0 \geq \sqrt{x_0}(s_0a_0+t_0b_0)$ is true.

2. Proof of $\underset{a,b,x}{\forall} \neg(0 < a \leq \sqrt{x} \leq b \wedge s_0a+t_0b = 0)$.

   We prove the contrapositive $\underset{a,b,x}{\exists}\ 0 < a \leq \sqrt{x} \leq b \wedge s_0a+t_0b = 0$. Take $a = -t_0$, $b = s_0$, $x = s_0$, $|t_0| \leq |s_0|$. We obtain $0 < -t_0 \leq s_0 \leq s_0 \wedge -s_0t_0+s_0t_0 = 0$, which is true.

" $\Longleftarrow$ ". Take a_0, b_0, x_0 arbitrary. Assume $0 < a_0 \leq \sqrt{x_0} \leq b_0$. Prove $\frac{p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0}{s_0a_0+t_0b_0} \leq \sqrt{x_0}$.

Instantiate in assumptions $a = a_0$, $b = b_0$, $x = x_0$, obtaining:

$0 < a_0 \leq \sqrt{x_0} \leq b_0 \wedge s_0a_0+t_0b_0 < 0 \Rightarrow p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0 \geq \sqrt{x_0}(s_0a_0+t_0b_0)$ and $\neg(0 < a_0 \leq \sqrt{x_0} \leq b_0 \wedge s_0a_0+t_0b_0 = 0)$.

Because $0 < a_0 \leq \sqrt{x_0} \leq b_0$ and $s_0a_0+t_0b_0 < 0$ are true, $\frac{p_0a_0^2+q_0a_0b_0+r_0b_0^2+x_0}{s_0a_0+t_0b_0} \leq \sqrt{x_0}$.

□

Lemma 12. *Prove that:*

$$\underset{p,q,r,s,t}{\forall} s > 0 \wedge t < 0 \wedge s+t = 0 \Longrightarrow \begin{bmatrix} \underset{a,b,x}{\forall} \neg(0 < a \leq \sqrt{x} \leq b \wedge sa+tb = 0) \Longleftrightarrow \\ false \end{bmatrix}$$

Proof. Take p_0, q_0, r_0, s_0, t_0 arbitrary. Assume $s_0 > 0$, $t_0 < 0$, $s_0+t_0 = 0$. Prove

$$\begin{bmatrix} \underset{a,b,x}{\forall} \neg(0 < a \leq \sqrt{x} \leq b \wedge s_0a+t_0b = 0) \Longleftrightarrow \\ false \end{bmatrix}.$$

" $\Longrightarrow$ ". We prove the contrapositive $\underset{a,b,x}{\exists}\ 0 < a \leq \sqrt{x} \leq b \wedge s_0a+t_0b = 0$. We take $a = -t_0$, $b = s_0$, $x = s_0$, $|t_0| \leq |s_0|$. We obtain $0 < -t_0 \leq s_0 \leq s_0 \wedge -s_0t_0+s_0t_0 = 0 = 0$, which is true.

" $\Longleftarrow$ ". Evidently true.

□