How the Main Program Proofs Work

Rich Schwartz

December 29, 2022

0.1 A Guide to the Techniques

The Lemmas in this part of the monograph deal with expressions of the form

$$C_Y(s) = \sum_{\alpha=0}^{E} s^\alpha (a_{2,\alpha} 2^{-s/2} + a_{3,\alpha} 3^{-s/2} + a_{4,\alpha} 4^{-s/2}). \tag{1}$$

Here

$$Y = (a_{2,0}, a_{3,0}, a_{4,0}, a_{2,1}, a_{3,1}, a_{4,1}, ...)$$

is a rational vector and $s \geq 0$. We call expressions in Equation 1 *power combos*. Our idea is to bound power combos by polynomials and then use positive dominance. To facilitate our polynomial approximation, we use interval valued polynomials. All this is explained in this document.

0.2 Positive Dominance

Positive Dominance is a positivity certificate that I discovered myself, though I wouldn't be surprised if it is in the literature.

Let $G \in \boldsymbol{R}[x_1, ..., x_n]$ be a multivariable polynomial:

$$G = \sum_I c_I X^I, \qquad X^I = \prod_{i=1}^{n} x_i^{I_i}. \tag{2}$$

Given two multi-indices I and J, we write $I \preceq J$ if $I_i \leq J_i$ for all i. Define

$$G_J = \sum_{I \preceq J} c_I, \qquad G_\infty = \sum_I c_I. \tag{3}$$

We call G *weak positive dominant* (WPD) if $G_J \geq 0$ for all J and $G_\infty > 0$.

Lemma 0.1 (Weak Positive Dominance) *If G is weak positive dominant then $G > 0$ on $(0,1]^n$.*

Proof: Suppose $n = 1$. Let $P(x) = a_0 + a_1 x + ...$ Let $A_i = a_0 + ... + a_i$. The proof goes by induction on the degree of P. The case $\deg(P) = 0$ is obvious. Let $x \in (0,1]$. We have

$$P(x) = a_0 + a_1 x + x_2 x^2 + \cdots + a_n x^n \geq$$
$$x(A_1 + a_2 x + a_3 x^2 + \cdots a_n x^{n-1}) = xQ(x) > 0$$

Here $Q(x)$ is WPD and has degree $n-1$.

Now we consider the general case. We write

$$P = f_0 + f_1 x_k + ... + f_m x_k^m, \qquad f_j \in \boldsymbol{R}[x_1, ..., x_{n-1}]. \tag{4}$$

Since P is WBP so are the functions $P_j = f_0 + ... + f_j$. By induction on the number of variables, $P_j > 0$ on $(0,1]^{n-1}$. But then, when we arbitrarily set the first $n-1$ variables to values in $(0,1)$, the resulting polynomial in x_n is WPD. By the $n = 1$ case, this polynomial is positive for all $x_n \in (0,1]$. ♠

Strong Positive Dominance: We call the polynomial P *positive dominant* if the inequalities in Equation 3 are all strict. In this case the same argument as above shows that $P > 0$ on the closed cube $[0,1]^n$.

Polynomial Subdivision: Let $P \in \boldsymbol{R}[x_1, ..., x_n]$ as above. Given an index j and a choice $k \in \{0,1\}$ we define the new polynomial $Q = S_{j,p}(P)$ by the formula

$$Q(x_1, ..., x_n) = P(x_1, ..., x_{i-1}, x_i^*, x_{i+1}, ..., x_n), \qquad x_i^* = \frac{k}{2} + \frac{x_i}{2}. \tag{5}$$

If $S_{i,k}(P) > 0$ on $(0,1]^n$ for $k = 0, 1$ then we also have $P > 0$ on $(0,1]^n$. As a matter of notation, we might sometimes write, say, $S_{d,k}$ in place of $S_{4,k}$ if we are using the variable names $(a, b, c, d) = (x_1, x_2, x_3, x_4)$. The operations $S_{d,0}$ and $S_{d,1}$ denote "subdivision along the d variable".

Positive Numerator Selection: If $f = f_1/f_2$ is a bounded rational function on $[0,1]^n$. written in so that f_1, f_2 have no common factors, we always choose f_2 so that $f_2(1, ..., 1) > 0$. If we then show, one way or another, that $f_1 > 0$ on $(0,1]^n$ we can conclude that $f_2 > 0$ on $(0,1]^n$ as well. The point is that f_2 cannot change sign because then f blows up. But then we can conclude that $f > 0$ on $(0,1]^n$. We write $\text{num}_+(f) = f_1$.

0.3 Positive Dominance Subdivision Algorithm

This section depends on the positive dominance criterion from §0.2. Let $F_1, ..., F_k$ be a list of polynomials defined on $[0,1]^D$ and let $S \subset [0,1]^D$. Consider the following algorithm.

1. Start with a list L of cubes. Initially $[0,1]^D$ is the only cube on the list.
2. If L is empty, then **HALT**. Otherwise let Q be the last member of L.
3. If any of $F_1, ..F_k$ is positive dominant on Q, or if $Q \cap S = \emptyset$, we delete Q from L and go to Step 2.
4. Otherwise we delete Q from L and append to L the 2^D cubes of its dyadic subdivision. Then we ago to to Step 2.

If this algorithm halts then $\max(F_1, ..., F_k) > 0$ on S. We have described this algorithm in great generality so that we only need to describe it once. In one application below we will have $k = D = 1$ and $S = [0, h]$. In the other application we will have $k = 4$ and $D = 2$ and $S = [0,1]^2$.

0.4 Interval Polynomials

We define a *rational interval* to be an interval of the form $I = [L, R]$ where $L, R \in \boldsymbol{Q}$ and $L \leq R$. As a notational convention we treat rational constants as intervals with the same endpoint. Thus $C = [C, C]$. We say that I *traps* $r \in \boldsymbol{R}$ if $r \in I$. For example, define

$$L_2 = \left[\frac{25469}{36744}, \frac{7050}{10171}\right], \quad L_3 = \left[\frac{5225}{4756}, \frac{708784}{645163}\right], \quad L_4 = \left[\frac{25469}{18372}, \frac{345197}{249007}\right]. \tag{6}$$

The interval L_m traps $\log m$ for $m = 2, 3, 4$.

For each operation $* \in \{+, -, \times\}$ we define

$$I_1 * I_2 = [\min(S), \max(S)], \qquad S = \{L_1 * L_2, L_1 * R_2, R_1 * L_2, R_2 * L_2\}. \tag{7}$$

Our operations are such that if I_j traps r_j for $j = 1, 2$ then $I_1 * I_2$ traps $r_1 * r_2$. We raise an interval to a positive integer power using iterated multiplication. These operations are commutative, associative, and distributive.

An *inteval polynomial* is an expression of the form $I_0 + I_1 t + ... + I_n t^n$, in which each coefficient is an interval and t is a variable meant to be taken in

$[0,1]$. Given the rules above, interval polynomials may be added, subtracted or multiplied, in the obvious way.

Let $\mathcal{P}$ be the above interval polynomial. We say that $\mathcal{P}$ *traps* the ordinary polynomial $C_0 + C_1 t + ... + C_n t^n$ of the same degree degree if $C_j \in I_j$ for all j. We define the *min* of an interval polynomial to be the polynomial whose coefficients are the left endpoints of the intervals. We define the *max* similarly. If $\mathcal{P}$ is an interval polynomial which traps an ordinary polynomial, then $\mathcal{P}_{\min}(t) \le P(t) \le \mathcal{P}_{\rm mat}(t)$ for all $t \ge 0$. Moreover, if $\mathcal{P}_j$ traps the polynomial P_j for $j = 1, 2$, then $\mathcal{P}_1 * \mathcal{P}_2$ traps $P_1 * P_2$. Here $* \in \{+, -, \times\}$.

0.5 Series Approximation for Power Functions

We take fairly high power series approximations so as to get good estimates. Let $m \in \{2, 3, 4\}$. Let $2k$ be an even integer. Let $s \in [2k-1, 2k+1]$. Taylor's Theorem with remainder gives us:

$$m^{-s/2} = \sum_{j=0}^{11} \frac{(-1)^j \log(m)^j}{m^k 2^j j!}(s-2k)^j + \frac{E_s}{12!}(s-2k)^{12}. \tag{8}$$

Here E_s is the remainder term. For all $s \ge 0$ we have

$$E_s = \frac{d^{12}}{ds^{12}} m^{-s/2} = \frac{m^{-s/2}\log(m)^{12}}{2^{12}} \in [0,1]. \tag{9}$$

With these bounds we can give an interval version of Equation 8:

$$A_m^{\pm}(t) = \sum_{j=0}^{11} \frac{(\mp 1)^j (L_m)^j}{m^k 2^j j!} t^j + I t^{12}, \quad I = [-1/12!, 1/12!]. \tag{10}$$

By construction $A_m^{\pm}(t)$ traps $m^{-s/2}$ when $s = 2k \pm t$ and $t \in [0,1]$.

Let C_Y be the power combo in Equation 1. We define

$$[Y, 2k, 2k \pm 1] = \Big(\sum_{\alpha=0}^{E} (2k \pm t)^{\alpha} (a_{2,\alpha} A_2^{\pm}(t) + a_{3,\alpha} A_3^{\pm}(t) + a_{4,\alpha} A_4^{\pm}(t)) \Big)_{\min}. \tag{11}$$

For each $2k = 0, ..., 16$, but excluding the interval $[-1, 0]$, we have

$$[Y, 2k, 2k \pm 1] \le C_Y(2k \pm t), \quad \forall t \in [0,1]. \tag{12}$$

Equation 12 bounds our power combos from below by rational polynomials.

0.6 Proof of the Lemmas

Here are alternate proofs of the lemmas from this part of the monograph.

Proof of Lemma A221: Let Y be the vector associated to any one of our coefficients $a_1(s), a_2(s), a_3(s), a_4(s)$. We show that $[Y, 0, 1]$ is weak positive dominant and $[Y, 2, 1], [Y, 2, 3], [Y, 4, 3], [Y, 4, 5], [Y, 6, 5]$ are positive dominant. This shows that $a_j(s) > 0$ for $a \in (0, 6]$. ♠

Proof of Lemma A222: We compute

$$11\psi_s(0) = \begin{bmatrix} -88 \\ -128 \\ +216 \\ +6 \\ +32 \\ +11 \end{bmatrix} \cdot \begin{bmatrix} 2^{-s/2} \\ 3^{-s/2} \\ 4^{-s/2} \\ s2^{-s/2} \\ s3^{-s/2} \\ s4^{-s/2} \end{bmatrix}, \qquad \frac{11}{s}\psi_s(4) = \begin{bmatrix} -2112 \\ +1664 \\ +459 \\ +219 \\ 288 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 2^{-s/2} \\ 3^{-s/2} \\ 4^{-s/2} \\ s2^{-s/2} \\ s3^{-s/2} \\ s4^{-s/2} \end{bmatrix}$$

Both expressions are power combos in the sense of Equation 1. We use the same methods as in the proof of Lemma A221 to show that these functions are positive for $s \in (0, 6]$. ♠

Proof of Lemma A231: We use the same method as in Lemma A221. In this case, all the polynomials are positive dominant. ♠

Proof of Lemma A232: We use the case $k = D = 1$ of the subdivision algorithm discussed in §0.3. For each relevant choice of Y we apply the algorithm to the functions $[Y, 13, 14], [Y, 14, 15], [Y, 16, 15]$ respectively on the sets $S = [0, 1]$, $[0, 1]$, $[0, h]$ where $h = \frac{25}{512}$. In all cases the algorithm halts. ♠

Proof of Lemma A233: We compute

$$33567\psi_s(0) = \begin{bmatrix} -88440 \\ -503040 \\ +591480 \\ +4254 \\ +65728 \\ +33567 \end{bmatrix} \cdot \begin{bmatrix} 2^{-s/2} \\ 3^{-s/2} \\ 4^{-s/2} \\ s2^{-s/2} \\ s3^{-s/2} \\ s4^{-s/2} \end{bmatrix}, \qquad \frac{33567}{s}\psi_s(4) = \begin{bmatrix} -48973248 \\ +32866944 \\ +16139871 \\ +4141935 \\ +8107680 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 2^{-s/2} \\ 3^{-s/2} \\ 4^{-s/2} \\ s2^{-s/2} \\ s3^{-s/2} \\ s4^{-s/2} \end{bmatrix}$$

The same method as above shows that these combos are positive for $s \in [6, 16]$. This shows that $\phi_s(0), \phi_s(4) > 0$ for all $s \in [6, 16]$.

Simple roots: Let $\psi_s' = d\psi_s/dr$. We need to show that ψ_s and ψ_s' do not have a common root. We define the functions

$$\phi_1(s,u) = \psi_s(r), \qquad \phi_2(s,u) = \psi_s'(r), \qquad r = 4u. \tag{13}$$

We make this change so that the u-variable ranges in $[0,1]$.

For each $j = 1,2$ and each interval $[6,7],[8,7],...[15,16]$ we construct polynomials $\underline{\phi}_j$ and $\overline{\phi}_j$ on $[0,1]^2$ such that

$$\phi_j(s',u) \geq \underline{\phi}_j(s,u), \qquad -\phi_j(s',u) \geq \overline{\phi}_j(s,u). \tag{14}$$

Here s' is a suitably translated version of s. Thus on the interval $[6,7]$ we have $s' = s - 6$. On the interval $[8,7]$ we have $s' = 8 - s$. And so on. We run algorithm from §0.3 on the list $\{\underline{\phi}_1, \overline{\phi}_1, \underline{\phi}_2, \overline{\phi}_2\}$ and we see in all 10 cases that the algorithm halts. This implies that one of $\psi_s(r)$ or $\psi_s'(r)$ is nonzero for each $r \in [0,4]$ and $s \in [6,16]$.

The functions: For $j = 1,2$ there are vectors $Y_{j,1}, ..., Y_{j,10}$ such that

$$\phi_j(s,u) = \sum_{\ell=0}^{10} C_{Y_{j,\ell}}(s) u^\ell, \qquad u \in [0,1]. \tag{15}$$

For $j = 1,2$ and for each interval $[2k \pm 1, 2k]$, with $2k = 8, ..., 16$, define

$$\underline{\phi}_j(t,u) = \sum_{\ell=0}^{10} [Y_{j,\ell}, 2k, 2k \pm 1](t) u^\ell, \qquad \overline{\phi}_j(t,u) = \sum_{\ell=0}^{10} [-Y_{j,\ell}, 2k, 2k \pm 1](t) u^\ell. \tag{16}$$

These functions have the desired properties. ♠