The Cauchy-Schwarz Inequality and Positive Polynomials

Torkel A. Haufmann

May 27, 2009

Contents

0.1 Introduction

This text consists of two parts. In chapter 1, we discuss the Cauchy-Schwarz inequality and some generalisations of this, in addition to looking at certain results related to said inequality. In chapter 2, we will instead turn our attention to positive polynomials, by their nature related to inequalities, and end with a characterisation of those positive polynomials that are sums of squares.

Chapter 1

The Cauchy-Schwarz Inequality

What is now known as the Cauchy-Schwarz inequality was first mentioned in a note by Augustin-Louis Cauchy in 1821, published in connection with his book *Course d'Analyse Algébrique*. His original inequality was formulated in terms of sequences in $\mathbb{R}$, but later Viktor Yakovlevich Bunyakovsky proved the analog version for integrals in his *Mémoire*(1859). In the course of his work on minimal surfaces Karl Hermann Amandus Schwarz in 1885 proved the inequality for two-dimensional integrals, apparently not knowing about Bunyakovsky's work. Due to Bunyakovsky's relative obscurity in the West at the time, the inequality came to be known as the Cauchy-Schwarz inequality, as opposed to, for instance, the Cauchy-Bunyakovsky-Schwarz inequality.

In keeping with mathematical tradition over historical precedence we will use the name Cauchy-Schwarz inequality, or CS inequality for short. As we will see, the inequality is valid in considerably more general cases than the ones thus far mentioned. We will not distinguish much between the different versions of the inequality, for our purposes they are all "the" CS inequality.

1.1 Initial proofs

This is the CS inequality as Cauchy originally discovered it:

Theorem 1.1.1 (CS inequality 1). *For two finite real sequences $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n$ the following holds:*

$$a_1b_1 + \cdots + a_nb_n \leq \sqrt{a_1^2 + \cdots + a_n^2}\sqrt{b_1^2 + \cdots + b_n^2}. \tag{1.1}$$

Direct proof. This first proof uses nothing but ordinary rules of algebra. Note that if either of the sequences are zero the CS inequality is trivial, so we assume this is not the case. We know that for all $x, y \in \mathbb{R}$,

$$0 \leq (x-y)^2 = x^2 - 2xy + y^2 \Rightarrow xy \leq \frac{1}{2}x^2 + \frac{1}{2}y^2 \tag{1.2}$$

Next, we introduce new normalised sequences, whose utility will become apparent, by defining

$$\hat{a}_i = a_i \Bigg/ \left(\sum_{j=1}^{n} a_j^2\right)^{\frac{1}{2}} \quad \text{and } \hat{b}_i = b_i \Bigg/ \left(\sum_{j=1}^{n} b_j^2\right)^{\frac{1}{2}}.$$

Applying 1.2 to these two sequences, term by term, it is clear that

$$\sum_{i=1}^{n} \hat{a}_i \hat{b}_i \leq \frac{1}{2}\sum_{i=1}^{n} \hat{a}_i^2 + \frac{1}{2}\sum_{i=1}^{n} \hat{b}_i^2 = \frac{1}{2} + \frac{1}{2} = 1.$$

Reintroducing the original sequences this means that

$$\sum_{i=1}^{n} \frac{a_i}{\left(\sum_{j=1}^{n} a_j\right)^{\frac{1}{2}}} \frac{b_i}{\left(\sum_{j=1}^{n} b_j\right)^{\frac{1}{2}}} \leq 1,$$

and as an immediate consequence,

$$\sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}},$$

thus finishing the proof. □

As a side note, observe that if the sums were infinite but convergent in the L_2-norm we could have performed the exact same proof above, but we have kept this proof simple so as not to obscure the idea.

The next proof we present will be due to viewing the finite sequences as vectors $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots b_n)$ in $\mathbb{R}^n$ or $\mathbb{C}^n$. We restate the properties of the inner product on a vector space V over some field $\mathbb{K}$ that is either $\mathbb{R}$ or $\mathbb{C}$:

$$\forall \mathbf{v}, \mathbf{v}', \mathbf{w} \in V, \forall c \in \mathbb{K}$$

1. $\langle \mathbf{v} + \mathbf{v}', \mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle + \langle \mathbf{v}', \mathbf{w} \rangle$
2. $\langle \mathbf{w}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{w} \rangle}$
3. $\langle c\mathbf{v}, \mathbf{w} \rangle = c\langle \mathbf{v}, \mathbf{w} \rangle$
4. $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0, \qquad \langle \mathbf{v}, \mathbf{v} \rangle = 0 \Rightarrow \mathbf{v} = \mathbf{0}$

Now we will define a norm on this space, which will enable us to prove the CS inequality again. Recall that a norm $\|\cdot\|$ on some vector space satisfies the following:

$$\forall \mathbf{v}, \mathbf{w} \in V, \forall c \in \mathbb{K}$$

1. $\|c\mathbf{v}\| = |c|\|\mathbf{v}\|$
2. $\|\mathbf{v}\| \geq 0$ and $\|\mathbf{v}\| \Rightarrow \mathbf{v} = \mathbf{0}$
3. $\|\mathbf{v}+\mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$
4. $|\langle \mathbf{v}, \mathbf{w}\rangle| \leq \|\mathbf{v}\|\|\mathbf{w}\|$

where we recognise property 4 as the CS inequality. Our next theorem essentially states that the standard norm defined as $\|\mathbf{v}\| = \langle \mathbf{v}, \mathbf{v}\rangle^{1/2}$ for $\mathbf{v} \in V$ has this property. That it satisfies the first two properties is easy to prove, so only the third is left. We will return to this later.

Theorem 1.1.2 (CS inequality 2)**.** *In a vector space V with an inner product $\langle \cdot, \cdot \rangle$ and the standard norm $\|\mathbf{v}\| = \langle \mathbf{v}, \mathbf{v}\rangle^{1/2}$ for $\mathbf{v} \in V$ the following holds for $\mathbf{a}, \mathbf{b} \in V$:*

$$|\langle \mathbf{a}, \mathbf{b}\rangle| \leq \|\mathbf{a}\|\|\mathbf{b}\|. \tag{1.3}$$

We will use the easily checked fact that $\|c\mathbf{v}\| = |c|\|\mathbf{v}\|$ for $c \in \mathbb{K}$, $\mathbf{v} \in V$. We will also use the notion of projection, and we remind the reader that for $\mathbf{w} \in V$, then the projection of $\mathbf{v} \in V$ onto the subspace spanned by $\mathbf{w}$ is defined by

$$\operatorname{Proj}_{\mathbf{w}}(\mathbf{v}) = \frac{\langle \mathbf{v}, \mathbf{w}\rangle}{\langle \mathbf{w}, \mathbf{w}\rangle}\mathbf{w}.$$

It is clear that there exists a $\mathbf{v}' \in V$ such that $\mathbf{v} = \operatorname{Proj}_{\mathbf{w}}(\mathbf{v}) + \mathbf{v}'$ and $\mathbf{v}, \mathbf{v}'$ are orthogonal. It's easy to verify that

$$\|\mathbf{v}\|^2 = \|\operatorname{Proj}_{\mathbf{w}}(\mathbf{v})\|^2 + \|\mathbf{v} - \operatorname{Proj}_{\mathbf{w}}(\mathbf{v})\|^2.$$

From this it is obvious that $\|\operatorname{Proj}_{\mathbf{w}}(\mathbf{v})\| \leq \|\mathbf{v}\|$, and we can exhibit the proof.

Proof. Assume $\mathbf{a} \neq 0$, otherwise the inequality is the trivial equality $0 = 0$. Now let W be the subspace spanned by $\mathbf{a}$. Then

$$\|\operatorname{Proj}_W \mathbf{b}\| = \left\| \frac{\langle \mathbf{a}, \mathbf{b}\rangle}{\langle \mathbf{a}, \mathbf{a}\rangle}\mathbf{a} \right\| = \frac{|\langle \mathbf{a}, \mathbf{b}\rangle|}{|\langle \mathbf{a}, \mathbf{a}\rangle|}\|\mathbf{a}\| = \frac{|\langle \mathbf{a}, \mathbf{b}\rangle|}{\|\mathbf{a}\|^2}\|\mathbf{a}\| = \frac{|\langle \mathbf{a}, \mathbf{b}\rangle|}{\|\mathbf{a}\|},$$

and since $\|\operatorname{Proj}_W \mathbf{b}\| \leq \|\mathbf{b}\|$ the theorem immediately follows. ☐

Now, this is all independent of how we have defined the inner product on V, thus leaving theorem 1.1.1 as a special case[1]. The proof is due to [2]. We could also have proved this using the method of normalisation from the proof of theorem 1.1.1, adapting notation as necessary, but we will not do that here.

Of particular interest is that Theorem 1.1.2 has $\mathbb{C}^n$ as a special case with the inner product on that space defined by

$$\langle \mathbf{z}, \mathbf{w}\rangle = z_1\overline{w_1} + \cdots + z_n\overline{w_n},$$

---

[1] Technically, the theorem is subtly different because of the absolute value on the left. This, however, presents no difficulty, as obviously, if $|x| \leq |y|$ then $x \leq |y|$ for all $x, y \in \mathbb{R}$.

and thus the CS inequality also holds for sequences in $\mathbb{C}$, provided the second sequence is complex conjugated as above.

In fact, this inner product form of the CS inequality is the most general form we will exhibit in this paper, and the fact that the CS inequality holds for any inner product space surely underlines how general the result truly is.

1.2 Some other cases

The CS inequality for integrals of functions into $\mathbb{R}$ is easily obtained for instance through taking limits on the discrete case – this is how Bunyakovsky originally proved it, though we might as well have proven it by defining an inner product on the space of integrable functions over some interval, leaving it as a special case of Theorem 1.1.2. We merely state it here without proof.

Theorem 1.2.1 (Bunyakovsky's Inequality). *Let $I \subset \mathbb{R}$ be an interval and assume we have two functions $f, g : I \to \mathbb{R}$ that are integrable on I. Then*

$$\int_I fg \leq \left(\int_I f^2 \right)^{\frac{1}{2}} \left(\int_I g^2 \right)^{\frac{1}{2}}. \tag{1.4}$$

That said, the twodimensional case, proven by Schwarz as mentioned, is more interesting. I now state the result and prove it, the proof is after [5].

Theorem 1.2.2 (CS Inequality 3). *Let $S \subset \mathbb{R}^2$, and assume we have two functions $f, g : S \to \mathbb{R}$ that are integrable on S. Then the following holds:*

$$\left| \iint_S fg \right| \leq \sqrt{\iint_S f^2} \sqrt{\iint_S g^2}. \tag{1.5}$$

Proof. Define the following three quantities:

$$A = \iint_S f^2, \qquad B = \iint_S fg, \text{ and} \qquad C = \iint_S g^2.$$

Then consider the following polynomial:

$$p(t) = \iint_S (tf(x, y) + g(x, y))^2 dxdy = At^2 + 2Bt + C.$$

$p(t)$ is nonnegative, being the integral of a square, and we know this means the discriminant of this polynomial must be less than or equal to 0, that is, $4B^2 - 4AC \leq 0$, implying $B^2 \leq AC$, which by taking roots immediately gives us Theorem 1.2.2. ☐

Again, this could have been just as easily proved by defining an inner product, illustrating again that Theorem 1.1.2 is by far the most general case of the CS inequality we discuss here. Note that this particular technique of proof can be reused, for instance to prove the analoguous discrete version.

Theorem 1.2.3 (CS Inequality 4)**.** *If $a_{i,j}$ and $b_{i,j}$ are two doubly indexed finite sequences such that $1 \leq i \leq m$ and $1 \leq j \leq n$, the following holds:*

$$\sum_{i,j} a_{i,j} b_{i,j} \leq \sqrt{\sum_{i,j} a_{i,j}^2} \sqrt{\sum_{i,j} b_{i,j}^2}. \tag{1.6}$$

where we implicitly asssume the double sums are over the full ranges of i and j.

Proof. In fact, this proof proceeds exactly analoguously to the proof of Theorem 1.2.2. Define

$$A = \sum_{i,j} a_{i,j}^2, \qquad B = \sum_{i,j} a_{i,j} b_{i,j}, \qquad C = \sum_{i,j} b_{i,j}^2.$$

Now we let

$$p(t) = \sum_{i,j} (t a_{i,j} + b_{i,j})^2 = At^2 + 2Bt + C$$

and the rest of the proof proceeds exactly as the earlier one. ☐

This could also have been proved by defining an appropriate inner product on the space of $m \times n$-matrices, so this too is a special case of Theorem 1.1.2.

1.3 Sharpness

I have not yet discussed sharpness of the inequality, that is, when it is in fact an identity. As it turns out the answer to this will be that the CS inequality is an equality in the case when the sequences are proportional, or, in the continuous case, when the functions are. This is, however, much more easily discussed in view of the Lagrange Identity, so I will postpone further discussion of the subject until then for the discrete case.

In the continuous case, however, we can learn this simply by looking at the polynomial we used in the proof of theorem 1.2.2. If there is some $t_0 \in \mathbb{R}$ such that $p(t_0) = 0$ then the discriminant is obviously zero, so that $B^2 = AC$. This means, however, that the integral is zero, and given that the integrand is nonnegative it, too, must be zero. So

$$|B| = \sqrt{A}\sqrt{B} \Longrightarrow t_0 f(x,y) + g(x,y) = 0,$$

and this last equality simply means the two functions are proportional.

1.4 Related results

As mentioned, the CS inequality is a very general inequality, and various related inequalities are found all the time. I've included some of these related results here. The first is due to [5].

Theorem 1.4.1 (Schur's Lemma)**.** *Given an $m \times n$-matrix A where $a_{i,j}$ denotes the element in the i-th row of the j-th column and two sequences $\{x_i\}_{i=1}^m$ and $\{y_j\}_{j=1}^n$ the following holds:*

$$\left|\sum_{i=1}^m \sum_{j=1}^n a_{i,j} x_i y_j\right| \leq \sqrt{RC} \sqrt{\sum_{i=1}^m |x_i|^2} \sqrt{\sum_{j=1}^n |y_j|^2},$$

where $R = \max_i \sum_{j=1}^n |a_{i,j}|, C = \max_j \sum_{i=1}^m |a_{i,j}|$, i.e. R is the largest absolute row sum, and C is the largest absolute column sum.

Proof. We split the summand into $|a_{i,j}|^{1/2}|x_i||a_{i,j}|^{1/2}|y_j|$, considering the first two terms to be one sequence, and the next two another. Then we use Theorem 1.2.3 on this product, obtaining

$$\begin{aligned}\left|\sum_{i=1}^m \sum_{j=1}^n a_{i,j} x_i y_j\right| &\leq \left(\sum_{i,j} |a_{i,j}||x_i|^2\right)^{1/2} \left(\sum_{i,j} |a_{i,j}||y_j|\right)^{1/2} \\ &= \left(\sum_{i=1}^m \left(\sum_{j=1}^n |a_{i,j}|\right) |x_i|^2\right)^{1/2} \left(\sum_{j=1}^n \left(\sum_{i=1}^m |a_{i,j}|\right) |y_j|\right)^{1/2} \\ &\leq \left(\sum_{i=1}^m R|x_i|^2\right)^{1/2} \left(\sum_{j=1}^n C|y_j|\right)^{1/2} \\ &= \sqrt{RC} \left(\sum_{i=1}^m |x_i|^2\right)^{1/2} \left(\sum_{j=1}^n |y_j|\right)^{1/2}. \qquad \square\end{aligned}$$

The next result is given in [1].

Theorem 1.4.2 (An additive inequality)**.** *If $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n, \{c_i\}_{i=1}^n, \{d_i\}_{i=1}^n$ are finite real sequences, and $\{p_i\}_{i=1}^n, \{q_i\}_{i=1}^n$ are nonnegative finite real sequences, the following holds:*

$$2\sum_{i=1}^n p_i a_i c_i \sum_{i=1}^n q_i b_i d_i \leq \sum_{i=1}^n p_i a_i^2 \sum_{i=1}^n q_i b_i^2 + \sum_{i=1}^n p_i c_i^2 \sum_{i=1}^n q_i d_i^2.$$

If the p_i and q_i are positive we have equality if and only if $a_i b_j = c_i d_j$ for all i, j.

Proof. Recall that if $a, b \in \mathbb{R}$ then

$$0 \leq (a-b)^2 \Rightarrow 2ab \leq a^2 + b^2$$

where equality is attained in the case $a = b$. Clearly, this means that for any $1 \leq i, j \leq n$ we have

$$2a_i c_i b_j d_j \leq a_i^2 b_j^2 + c_i^2 d_j^2$$

and equality if and only if $a_i b_j = c_i d_j$. Since $p_i q_j \geq 0$ we can now multiply both sides of this equation with this, obtaining

$$2p_i q_j a_i c_i b_j d_j \leq p_i q_j a_i^2 b_j^2 + p_i q_j c_i^2 d_j^2$$

We sum over both i and j and collect terms, thus obtaining

$$2\sum_{i=1}^{n} p_i a_i c_i \sum_{i=1}^{n} q_i b_i d_i \leq \sum_{i=1}^{n} p_i a_i^2 \sum_{i=1}^{n} q_i b_i^2 + \sum_{i=1}^{n} p_i c_i^2 \sum_{i=1}^{n} q_i d_i^2$$

which is our desired inequality. If either the p_i or q_j are ever zero there are no bounds on the corresponding terms in the other four sequences, so if we want to say something in general about equality, we have to assume $p_i, q_j > 0$ for all i, j, in which case it's clear that we have equality only if all the inequalities we sum over have equality, which means that for any i, j we must have $a_i b_j = c_i d_j$. $\square$

It may not be immediately obvious how the last inequality relates to the CS inequality, but consider choosing $p_i = q_i = 1$ for all i, $c_i = b_i$ and $d_i = a_i$. Then the inequality reduces to

$$2\sum_{i=1}^{n} a_i b_i \sum_{i=1} b_i a_i \leq \sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2 + \sum_{i=1}^{n} b_i^2 \sum_{i=1}^{n} a_i^2$$

which is readily seen to reduce to the standard CS inequality, and so theorem 1.4.2 is in fact a generalisation.

Next we tie up a loose end.

Theorem 1.4.3. *On an inner product space V with inner product denoted by $\langle \cdot, \cdot \rangle$, the standard norm $\| \cdot \| = \langle \cdot, \cdot \rangle^{1/2}$ is a norm.*

Proof. We have seen that this standard norm possesses three of the four required properties (See the discussion preceding Theorem 1.1.2 – property 1 and 2 are trivial). We prove that it also possesses property 3, the triangle inequality.

We shall consider $\|\mathbf{a} + \mathbf{b}\|^2$ with $\mathbf{a}, \mathbf{b} \in V$. We can merely take square roots to obtain the desired result afterwards.

$$\begin{aligned} \|\mathbf{a} + \mathbf{b}\|^2 = \langle \mathbf{a} + \mathbf{b}, \mathbf{a} + \mathbf{b} \rangle &= \langle \mathbf{a}, \mathbf{a} \rangle + 2\langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{b}, \mathbf{b}, \rangle \\ &\leq \|\mathbf{a}\|^2 + 2\|\mathbf{a}\|\|\mathbf{b}\| + \|\mathbf{b}\|^2 \\ &= (\|\mathbf{a}\| + \|\mathbf{b}\|)^2 \end{aligned}$$

where the inequality is due to the CS inequality. The CS inequality therefore ensures the triangle inequality. $\square$

A final matter worthy of mention is that the CS inequality can be used to define the concept of angle on any real inner product space, by stating that if $(V, \langle \cdot, \cdot \rangle)$ is the space in question, $\| \cdot \|$ is the standard norm on V and $\mathbf{x}, \mathbf{y} \in V$ then defining

$$\cos\theta = \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|\|\mathbf{y}\|}$$

immediately ensures that $\cos\theta \in [-1, 1]$ and is 1 or -1 only if the vectors are proportional, as expected, and so this is a workable definition of the angle between $\mathbf{x}$ and $\mathbf{y}$.

1.5 Lagrange's Identity

Lagrange's Identity(LI) is an identity discovered by Joseph Louis Lagrange, which to us is mostly interesting for what it can tell us about the version of the CS inequality stated in theorem 1.1.1.

Theorem 1.5.1 (Lagrange's Identity). *For two real sequences $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n$ we have*

$$\left(\sum_{i=1}^n a_i b_i\right)^2 = \sum_{i=1}^n a_i^2 \sum_{i=1}^n b_i^2 - \frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n (a_i b_j - a_j b_i)^2. \tag{1.7}$$

Proof. The theorem is easily verified simply by expanding sums. I offer a quick rundown here, as this is more tedious than difficult:

$$\begin{aligned}\left(\sum_{i=1}^n a_i b_i\right)^2 &= \sum_{i=1}^n a_i b_i \sum_{j=1}^n a_j b_j \\ &= \sum_{i=1}^n\sum_{j=1}^n a_i b_i a_j b_j\end{aligned}$$

Using that $(a_i b_j - a_j b_i)^2 = a_i^2 b_j^2 - 2a_i b_i a_j b_j + a_j^2 b_i^2$ it's clear that

$$\begin{aligned}\left(\sum_{i=1}^n a_i b_i\right)^2 &= \frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n \left(a_i^2 b_j^2 + a_j^2 b_i^2 - (a_i b_j - a_j b_i)^2\right) \\ &= \frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n (a_i^2 b_j^2 + a_j^2 b_i^2) - \frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n (a_i b_j - a_j b_i)^2 \\ &= \sum_{i=1}^n\sum_{j=1}^n a_i^2 b_j^2 - \frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n (a_i b_j - a_j b_i)^2 \\ &= \sum_{i=1}^n a_i^2 \sum_{i=1}^n b_i^2 - \frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n (a_i b_j - a_j b_i)^2,\end{aligned}$$

and we're finished. □

Now, the interesting property of Lagrange's Identity, at least for us, is that it gives us the CS inequality with an error estimate.

Estimating the error in CS. Note that in Lagrange's Identity, the right-hand sum

$$\frac{1}{2}\sum_{i=1}^n\sum_{j=1}^n (a_i b_j - a_j b_i)^2$$

is surely nonnegative, as it is a sum of squares. Therefore, subtracting it must decrease the value of the right-hand side(Or leave it as it is, in the case the term is zero), and from this it follows that

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2,$$

and taking square roots

$$\left|\sum_{i=1}^{n} a_i b_i\right| \leq \sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2},$$

thus proving Theorem 1.1.1 again (This is perhaps the proof we've seen that best optimises the trade-off between speed and using simple concepts).

Further, it is clear that the two sides of the CS inequality are only equal in the case that the sum is zero, which means that

$$\forall i, j \qquad a_i b_j - a_j b_i = 0 \Leftrightarrow a_i b_j = a_j b_i \Leftrightarrow \frac{a_i}{a_j} = \frac{b_i}{b_j}$$

i.e. the two sequences are proportional. □

Thus, the quadratic term $\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}(a_i b_j - a_j b_i)^2$ is a measure of the error in the CS inequality as it is stated in theorem 1.1.1.

We take note that Lagrange's identity automatically generates positive polynomials, as it writes them as a sum of squares. We might begin to wonder whether this is something that can be done in general, i.e. if most or all positive polynomials may be written as sums of squares. I will discuss this matter in the next chapter.

Chapter 2

Positive polynomials

In the rest of this text, we will concern ourselves with the representation of positive polynomials, taking this to mean any polynomial that is never negative (Technically, a non-negative polynomial). Note that we only consider real polynomials. We shall need the following two definitions.

Definition 2.0.2 (Positivity of a polynomial)**.** *If p is a polynomial we shall take $p \geq 0$ to mean that p is never negative. We shall occasionally say that p is* positive *if $p \geq 0$.*

Definition 2.0.3 (Sum of squares)**.** *We shall say that p is a sum of squares if we can write $p = p_1^2 + \cdots + p_n^2$ for some n and where p_i is a polynomial for $i = 1, \dots, n$. We will use* **sos** *as shorthand for sum of squares.*

Obviously, p is **sos** $\Rightarrow p \geq 0$. It's not, however, immediately obvious that $p \geq 0 \Rightarrow p$ is **sos**, and in fact this is not the case – this is known as Minkowski's Conjecture after Charles Minkowski (The correct implication was proven by Artin in 1928, and we will get back to this later).

An example of a positive polynomial that can't be written as a sum of squares was originally given by Motzkin in 1967, and we reproduce it as stated in [3]. If we define $s(x, y) = 1 - 3x^2y^2 + x^2y^4 + x^4y^2$ then this polynomial is positive (see Figure 2.1), but it's not a sum of squares, this claim will be proved later.

Now, two questions arise. First, what characterises those polynomials that *are* sums of squares? Second, what is the correct characterisation of positive polynomials? We investigate the first question first, and then we conclude by showing the answer to the second.

2.1 Sums of squares

2.1.1 Polynomials in one variable

One thing that is easy to prove is that any second-degree positive polynomial in one variable can be written as a sum of squares. We do as follows, completing

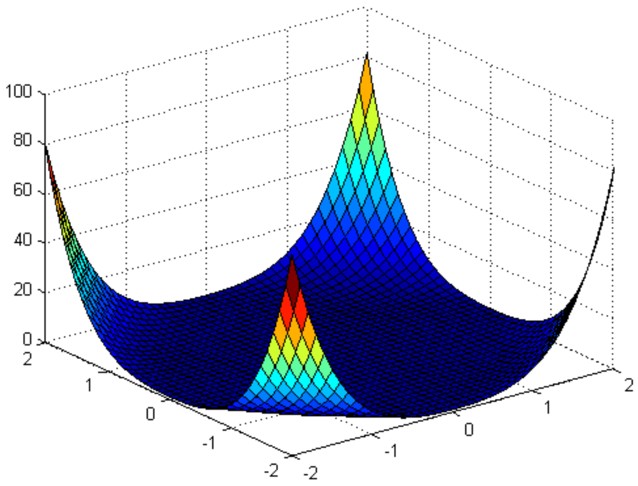

Figure 2.1: A positive polynomial that isn't **sos**.

the square:

$$p(x) = ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a}$$

Now, obviously we must have $a \geq 0$ in order to have $p \geq 0$. Also, it's clear that $p(-b/2a)$ should also be nonnegative, and this directly implies that $4ac - b^2 \geq 0$. As both of the terms on the right are nonnegative we can take their square roots, thus obtaining

$$p_1(x) = \sqrt{a}\left(x + \frac{b}{2a}\right), \qquad p_2(x) = \frac{\sqrt{4ac - b^2}}{2\sqrt{a}},$$

allowing us to write

$$p = p_1^2 + p_2^2.$$

We can in fact expand this to be correct for polynomials of any degree, provided we do not add further variables.

Theorem 2.1.1. *If p is a polynomial in one variable, then $p \geq 0 \Leftrightarrow p$ is* **sos**. *Also, $p \geq 0$ means that $p = p_1^2 + p_2^2$ for some polynomials p_1, p_2.*

Proof. p is **sos** $\Rightarrow p \geq 0$ was noted earlier to be evidently true. We prove the other implication, following [5]. If q_1, q_2, r_1, r_2 are polynomials, it is trivial to check that

$$(q_1^2 + q_2^2)(r_1^2 + r_2^2) = (q_1 r_1 + q_2 r_2)^2 + (q_1 r_2 - q_2 r_1)^2.$$

In other words, if $q = q_1^2 + q_2^2$ and $r = r_1^2 + r_2^2$ are both sums of two squared polynomials, then $p = qr$ is also a sum of two squares of polynomials.

We assume that p is a polynomial of some degree greater than two that is never negative. We intend to factor p into positive polynomials of degree two; then the above identity will show us that p is certainly a sum of two squares of polynomials.

We split this into two cases. First, we assume p has a real root r of multiplicity m. Then

$$p(x) = (x - r)^m q(x) \text{ where } q(r) \neq 0.$$

Now we need to prove that m is even. We focus our attention on a neighbourhood of r, setting $x = r + \epsilon$. Then $p(x + \epsilon) = \epsilon^m q(r + \epsilon)$. q is a polynomial and thus continuous so there exists a $\delta > 0$ so $q(r + \epsilon)$ doesn't change sign as long as $|\epsilon| \leq \delta$. Given that p is positive it should be clear that then obviously ϵ^m must have the same sign for all $|\epsilon| \leq \delta$, in particular even if it is negative, so m must be even. Then clearly $(x - r)^m$ is a positive polynomial, and so if p is to be positive q must be as well, and we have factored p into a product of two positive polynomials of lower degree than p.

The other possible situation is that p has no real roots. If so, let r and $\bar{r}$ be two conjugate complex roots. Then we can write

$$p(x) = (x - r)(x - \bar{r})q(x),$$

where obviously $(x - r)(x - \bar{r})$ has no real roots, is positive for large x, and as such is always positive on the real line. It follows that in order for p to be positive q has to be positive as well. Thus we have factored p into a product of two positive polynomials of lower degree than p again.

We have proven that if p is a polynomial and $p \geq 0$, it can be factored repeatedly by the two arguments above until it is a product of positive polynomials of degree two (Our arguments hold for any polynomial of degree greater than two, so we merely proceed by induction). Technically, we require here that the degree of p is even, but if it is not we can't possibly have $p \geq 0$, so this presents no difficulty. As shown initially, each of these second-degree terms is a **sos** of two squares, and using the initial identity and induction again we obtain a representation of their product as a **sos** of two squares. $\square$

2.1.2 Motzkin's polynomial revisited

Expanding the type of polynomials under consideration to those dependent on several variables the situation is no longer that simple. We revisit the polynomial $s(x, y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 1$ discussed initially. We prove that this is a positive polynomial. If we take the means of x^2, y^2 and $1/x^2y^2$ we observe that by the AM-GM inequality

$$\begin{aligned}
1 = \left(\frac{x^2y^2}{x^2y^2}\right)^{\frac{1}{2}} &\leq \frac{1}{3}\left(x^2 + y^2 + \frac{1}{x^2y^2}\right) \\
3x^2y^2 &\leq x^4y^2 + x^2y^4 + 1 \\
0 &\leq x^4y^2 + x^2y^4 - 3x^2y^2 + 1.
\end{aligned}$$

Thus, $s \geq 0$, and we need to prove that it cannot be a sum of squares. We assume, for a contradiction, it is and write it as

$$s(x, y) = q_1^2(x, y) + q_2^2(x, y) + \cdots + q_n^2(x, y),$$

Since s has degree 6 none of the q_i can have degree higher than 3. Furthermore,

$$\begin{aligned}
s(x, 0) &= q_1^2(x, 0) + \cdots + q_n^2(x, 0) = 1 \text{ and} \\
s(0, y) &= q_1^2(0, y) + \cdots + q_n^2(0, y) = 1,
\end{aligned}$$

meaning that if either of the variables vanish the q_i must be constant. Thus we may keep only the "cross" terms, giving

$$q_i(x, y) = a_i + b_ixy + c_ix^2y + d_ixy^2.$$

It's clear when squaring this that the coefficient of x^2y^2 in q_i^2 is b_i^2. Then the coefficient of the sum of squares must be $b_1^2 + b_2^2 + \cdots + b_n^2$, which is obviously positive. However, our coefficient above was negative! Thus, s can't be **sos**.

2.2 Quadratic forms

The concept of positive semidefiniteness is related to that of positive polynomials. We explore this, following [2]. Consider the quadratic form $q(\mathbf{x})$ where $\mathbf{x}$ is a column vector of n indeterminates and $A \in M_{n\times n}(\mathbb{R})$ is a symmetric matrix

$$q(\mathbf{x}) = \mathbf{x}^T A\mathbf{x}. \tag{2.1}$$

If $q \geq 0$ in this case, we say that A is positive semidefinite, or **psd**.

Definition 2.2.1 (Change of variable). *If* $\mathbf{x}$ *is vector of indeterminates in* $\mathbb{R}^n$ *then a change of variable is defined by an equation of the form* $\mathbf{x} = P\mathbf{y}$ *where* P *is invertible and* $\mathbf{y}$ *is a new vector of indeterminates in the same space. Note that this is essentially a coordinate change.*

Theorem 2.2.2 (The Principal Axes theorem). *Given a quadratic form as in 2.1 we can introduce a change of variable* $\mathbf{x} = P\mathbf{y}$ *such that* $\mathbf{x}^T A\mathbf{x} = \mathbf{y}^T D\mathbf{y}$ *where* D *is diagonal, i.e. we have no cross-product terms. Note that the eigenvalues of* A *will be appearing on the diagonal of* D*.*

Proof. It is known from the Spectral Theorem(see [2]), that we do not have room to prove here, that a symmetric matrix is orthogonally diagonalizable, and we let P be the matrix that obtains this. Then $P^T = P^{-1}, P^{-1}AP = D$ where D is symmetric, and if we let $\mathbf{y}$ satisfy $\mathbf{x} = P\mathbf{y}$ then

$$\mathbf{x}^T A\mathbf{x} = \mathbf{y}^T P^T AP\mathbf{y} = \mathbf{y}^T D\mathbf{y}$$

thus finishing the proof. ☐

Now we prove the aforementioned assertion. We know that A has n eigenvalues, counting multiplicities, by the Spectral Theorem, and the following holds.

Theorem 2.2.3. *If A is* **psd** *then all eigenvalues of A are nonnegative.*

Proof. Using theorem 2.2.2 we obtain a variable change $\mathbf{x} = P\mathbf{y}$ such that

$$q(\mathbf{x}) = \mathbf{y}^T D\mathbf{y} = \lambda_1 y_1^2 + \cdots + \lambda_n y_n^2.$$

Now, since A is **psd** this is nonnegative by definition, and so we must have $\lambda_i \geq 0$ for all i. ☐

We can now prove the following:

Theorem 2.2.4. *If A is* **psd** *and q is as before then q is* **sos**.

Proof. By the proof of theorem 2.2.3 we actually obtain just the sum of squares representation we're looking for (since each y_i is a polynomial in some of the x_j) by taking roots of the eigenvalues (This can be done since they're not negative) and taking them inside the squares. ☐

We have proven a connection between positive semidefinite matrices and sums of squares. Unfortunately, quadratic forms as defined only encapsulate polynomials of second degree. If we are to prove a more general result about sums of squares we need to generalise this notion somewhat. That is what we're going to do next.

2.3 Final characterisation of sums of squares

The theorem we will prove in this section was originally proven by Choi, Lam and Reznick, but we will state and prove it as in [4] - though we do not include the entire discussion from that article, as it's not necessary for our purposes. We must first agree on some notation, again due to [4].

We consider polynomials in n variables $x_1, \ldots, x_n$ for some fixed n. We let $\mathbb{N}_0$ denote the set $\{0, 1, \ldots\}$. If $\alpha = (\alpha_1, \ldots, \alpha_n)$ we define, for notational convenience, $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$. We now let m be some nonnegative integer and define $\Lambda_m = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n : \sum_{i=1}^n \alpha_i \leq m\}$, that is, Λ_m is the set of all possible vectors α such that x^α is a polynomial of degree less than or equal to m. Thus, every polynomial p of degree less than or equal to m can be written as a weighted sum of these:

$$p(x_1, \ldots, x_n) = \sum_{\alpha \in \Lambda_m} a_\alpha x^\alpha$$

where the a_α are weights. Finally, we order the elements of Λ_m in some way, i.e. we write $\Lambda_m = \{\beta_1, \ldots, \beta_k\}$ provided $|\Lambda_m| = k$ (It's obvious from the definition that Λ_m is finite, and the nature of the order doesn't really matter as long as there is an order).

All that said, we can state the theorem we need.

Theorem 2.3.1 (Characterisation of Sums of Squares)**.** *If p is some polynomial in n variables and is of degree $2m$, then p is* **sos** *if and only if there exists a real, symmetric,* **psd** *matrix $B \in \mathbb{R}^{k \times k}$ such that*

$$p(x_1, \ldots, x_n) = \overline{\mathbf{x}}^T B \overline{\mathbf{x}}$$

where $\overline{\mathbf{x}}$ is the column vector with $k = |\Lambda_m|$ entries whose elements are x^{β_i} for $i = 1, \ldots, k$.

A small note: We won't always actually need the k entries to represent the polynomial – their weights may be zero. To prove the theorem we need the following lemma(see [2]).

Lemma 2.3.2. *If A is a real $m \times n$-matrix, $A^T A$ is* **psd***.*

Proof. Clearly, $A^T A$ is symmetric, since $(A^T A)^T = A^T (A^T)^T = A^T A$. Now consider the quadratic form $\mathbf{x}^T A^T A \mathbf{x}$. It's clearly true that

$$\mathbf{x}^T A^T A \mathbf{x} = (A\mathbf{x})^T (A\mathbf{x}) = \|A\mathbf{x}\|^2 \geq 0$$

under the usual norm on $\mathbb{R}^n$, and this means that A is **psd**. $\square$

We can now prove our main result.

Proof of theorem 2.3.1. First, assume p is **sos** of degree $2m$, and we need, say, t squares. Then $p = \sum_{i=1}^t q_i^2$ where for all i, $\deg(q_i) \leq m$. Let Λ_m be ordered as before, and $\mathbf{x}$ be as in the statement of the theorem. We let A be the $k \times t$-matrix with ith column equal to the coefficients of q_i with respect to our ordering of Λ_m. Then clearly

$$p = \sum_{i=1}^t q_i^2 \Rightarrow p = \overline{\mathbf{x}}^T A^T A \overline{\mathbf{x}}.$$

If we let $B = A^T A$ then clearly B is symmetric(and since A is real B is real), and it also has to be **psd** by lemma 2.3.2. Thus, we have proven one implication.

We next assume that p may be written as

$$p = \overline{\mathbf{x}} B \overline{\mathbf{x}}^T$$

where B is real, symmetric and **psd**. As B is symmetric it has k eigenvalues, counting multiplicities. Using the Spectral Theorem ([2]) there exists an orthogonal matrix V such that $B = VDV^T$ where D is the diagonal matrix with the eigenvalues $\lambda_1, \ldots, \lambda_k$ of B on its diagonal. Given that B is **psd**, then $\lambda_i \geq 0$ for all i. Now

$$p = \overline{\mathbf{x}}^T V^T D V \overline{\mathbf{x}}.$$

Define q_i to be the i-th element of $V\overline{\mathbf{x}}$. Now this is a quadratic form in the vector $(q_1, \ldots, q_k)^T$ with a diagonal matrix, and we have already seen that this is a sum of squares in the previous section – simply write out the product and take the square roots of the eigenvalues on the diagonal of D to bring them inside the polynomials (These roots can be taken as the eigenvalues are nonnegative). We have constructed a sum of squares, proving that p is **sos**. Note also that if λ_i is zero, q_i is also zero, so the only q_i we will use are the ones corresponding to positive eigenvalues of B. $\square$

We have found a complete characterisation of positive polynomials that are sums of squares.

2.3.1 An illustrating example

Theorem 2.3.1 may look a little involved, so we include an example to illustrate how it works in a two-variable case. Consider the following polynomial:

$$f(x, y) = x^4 + y^4 - 2x^2y + 3x^2 + 3y^2 + 2x + 1.$$

This arises by letting $f(x, y) = (x^2 - y)^2 + (x + y)^2 + (x - y)^2 + (y^2)^2 + (x + 1)^2$, that is, it is a sum of 5 squares. We define

$$\begin{aligned}
q_1(x, y) &= x^2 - y \\
q_2(x, y) &= x + y \\
q_3(x, y) &= x - y \\
q_4(x, y) &= y^2 \\
q_5(x, y) &= x + 1.
\end{aligned}$$

All of these have degree less than or equal to 2, so we consider

$$\Lambda_2 = \{(0, 0), (1, 0), (0, 1), (1, 1), (2, 0), (0, 2)\}.$$

If we define $\overline{\mathbf{x}}$ as above, then

$$\overline{\mathbf{x}} = (1, x, y, xy, x^2, y^2)^T.$$

We define A to be the matrix with rows equal to the coefficients of the q_i as in the proof of theorem 2.3.1. Then we get

$$A = \begin{bmatrix} 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } A^T A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

so defining $B = A^T A$ it's clear that B is real and symmetric, and it's **psd** by construction according to Lemma 2.3.2. By calculation, $\overline{\mathbf{x}}^T B \overline{\mathbf{x}} = 1 + 2x + 3x^2 + 3y^2 - 2x^2 y + x^4 + y^4 = f(x,y)$. Thus $f(x,y) = \overline{\mathbf{x}}^T B \overline{\mathbf{x}}$, illustrating one implication in theorem 2.3.1.

Doing this the other way is a little more involved, since diagonalising matrices of this size is troublesome by hand (In a practical implementation, some computer program would most likely be used). Therefore we will use another polynomial to illustrate this. Assume $\overline{\mathbf{x}} = (1, x, y)^T$ and

$$B = \begin{bmatrix} 6 & -2 & 1 \\ -2 & 6 & -1 \\ -1 & -1 & 5 \end{bmatrix},$$

and that we are given $f(x,y) = \overline{\mathbf{x}}^T B \overline{\mathbf{x}} = 6x^2 + 5y^2 - 2xy - 4x - 2y + 6$. Clearly B is symmetric and real, we want to find if it is **psd**. By calculation, the eigenvalues of B are $\lambda_1 = 8, \lambda_2 = 6$ and $\lambda_3 = 3$, so it is in fact positive definite – this is more than enough. In order to diagonalise B as done in the proof of the theorem, we calculate the eigenvectors and normalize them, getting

$$\mathbf{v}_1 = \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{bmatrix}, \qquad \mathbf{v}_2 = \begin{bmatrix} -1/\sqrt{6} \\ -1/\sqrt{6} \\ 2/\sqrt{6} \end{bmatrix} \text{ and } \qquad \mathbf{v}_3 = \begin{bmatrix} 1/\sqrt{6} \\ 1/\sqrt{6} \\ 1/\sqrt{6} \end{bmatrix}$$

Defining $V = [\mathbf{v}_1\, \mathbf{v}_2\, \mathbf{v_3}]$ and $D = \operatorname{diag}(8, 6, 3)$, it's clear that $B = VDV^T$, as required. We now define, as in the proof,

$$\begin{aligned} q_1 &= \sqrt{8}\left(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}x\right) = -2 + 2x, \\ q_2 &= \sqrt{6}\left(-\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{6}}x + \frac{2}{\sqrt{6}}y\right) = -1 - x + 2y, \\ q_3 &= \sqrt{3}\left(\frac{1}{\sqrt{3}} + \frac{1}{\sqrt{3}}x + \frac{1}{\sqrt{3}}y\right) = 1 + x + y, \end{aligned}$$

and it is easy to calculate that $q_1^2 + q_2^2 + q_3^2 = 6x^2 + 5y^2 - 2xy - 2y - 4x + 6 = f(x,y)$, thus giving us a representation as a sum of three squares. This concludes the illustration of the other implication in the proof.

2.4 Hilbert's 17th problem

In 1900 David Hilbert held a speech outlining 23 problems he considered to be fruitful questions for mathematicians of that time. The 17th problem is the one that has been under discussion here, and essentially it's a conjecture by Hilbert – namely that any positive polynomial can be written as a sum of squares of *rational* functions. As it turns out, this is the correct defining property of positive polynomials.

Hilbert's conjecture was resolved affirmatively in 1928 by Emil Artin, and the proof is considered one of the greatest triumphs of modern algebra. It uses a number of results beyond what we have room for here, though, and so we shall not attempt to reproduce it – it's given for instance in [3].

For instance the problematic polynomial $s(x,y) = 1 - 3x^2y^2 + x^2y^4 + x^4y^2$ we considered earlier can indeed be written as a sum of squares of rational functions, as required by Artin's result. It is done in the following way, due to [3]:

$$\begin{aligned} 1 - 3x^2y^2 + x^2y^4 + x^4y^2 &= \left(\frac{x^2y(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy^2(x^2+y^2-2)}{x^2+y^2}\right)^2 \\ &\quad + \left(\frac{xy(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{x^2-y^2}{x^2+y^2}\right)^2. \end{aligned}$$

Note also that in 1967 it was proven by Pfister(see [3]) that if p is a positive polynomial in n variables then 2^n squares will always be enough. It will often be possible, however, to write p as a sum of more squares than that. Note that the representation of Motzkin's polynomial above illustrates this, using $2^2 = 4$ squares.

Bibliography

[1] S. S. Dragomir. A survey on cauchy–bunyakovsky–schwarz type discrete inequalities. *Journal of Inequalities in Pure and Applied Mathematics*, 4, 2003.

[2] David C. Lay. *Linear Algebra and its Applications, 3rd ed.* Pearson Education, 2006.

[3] Murray Marshall. *Positive Polynomials and Sums of Squares.* American Mathematical Society, 2008.

[4] Victoria Powers and Thorsten Wörmann. An algorithm for sums of squares of real polynomials. *Journal of pure and applied algebra*, 127:99–104, 1998.

[5] J. Michael Steele. *The Cauchy-Schwarz Master Class.* Cambridge University Press, 2004.