Asymptotic and Catalytic Resource Orderings: Beyond Majorization

Tobias Fritz

December 2019

Overview

- Asymptotic and catalytic majorization
- The algebraic structure of resource theories
- Real algebra and Positivstellensätze
- A **new Positivstellensatz** for asymptotic and catalytic orderings
- Application to (matrix) majorization and random walks
- Getting rid of ε

Submajorization

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$ be vectors with entries in $\mathbb{R}_+$.

Definition

x **submajorizes** y, denoted $x \succ_w y$, if

$$\sum_{i=1}^{k} x_i \geq \sum_{i=1}^{k} y_i \qquad \forall k,$$

assuming decreasing rearrangement, $x_1 \geq \ldots \geq x_n$ and $y_1 \geq \ldots \geq y_m$, and padding with 0's if necessary.

- $x \succ_w y$ iff there is doubly substochastic matrix R such that $y = Rx$ (up to padding 0's).
- **Majorization** $x \succ y$ defined as $x \succ_w y$ and $\sum_i x_i = \sum_i y_i$.
- Characterizes pure-state LOCC via **Nielsen's theorem**.

- It is useful to have **monotones** to detect (non-)majorization.
- The **Rényi entropies** for $\alpha \in \mathbb{R} \cup \{\pm\infty\}$ and normalized x,

$$H_\alpha(x) := \frac{1}{1-\alpha} \log \left(\sum_i x_i^\alpha \right),$$

  are great monotones!
- Special cases:
  - $H_0(x) = \log |\mathrm{supp}(x)|$.
  - Shannon entropy $H_1(x) = -\sum_i x_i \log x_i$.
  - Min-entropy $H_\infty(x) = -\log \max_i x_i$.
  - Max-entropy $H_{-\infty}(x) = -\log \min_i x_i$.

The Rényi entropies detect **catalytic majorization**:

Theorem (Klimesh '07, Turgut '07, modulo subtleties)

If $\sum_i x_i = \sum_i y_i$ and $H_\alpha(x) < H_\alpha(y)$ for all α, then there is z with

$$x \otimes z \succ y \otimes z.$$

and **asymptotic majorization**:

Theorem (TF '15, Jensen '18)

Under similar hypotheses,

$$x^{\otimes n} \succ y^{\otimes n}$$

Goal: prove statements like this **for resource theories in general**!

The algebraic structure of resource theories

Definition

A **preordered semiring** S is a set with binary operations

$$+, \cdot \; : \; S \times S \longrightarrow S$$

satisfying the usual axioms with neutral elements 0 and 1, and a preorder relation $\geq$ such that

$$x \geq y \quad \Longrightarrow \quad x + z \geq y + z, \qquad xz \geq yz.$$

Interpretation:

- Preorder $\geq$: convertibility relation between resource objects.
- Multiplication $\cdot$: combination of resource objects.
- Addition $+$: often little resource-theoretic interpretation, but mathematically extremely useful.

- Example: quantum channels under direct sum and tensor product.
- The vectors $x \in \mathbb{R}_+^d$ form a preordered semiring Major:
  - with **direct sum** and **tensor product** as algebraic operations, and
  - submajorization $\succ_w$ as preorder.
- Example: compactly supported probability measures on $\mathbb{R}$, with
  - with sum and convolution as algebraic operations, and
  - the **stochastic order** as preorder.

  Think: distribution of work in thermodynamics.

- The ℓ^p-norms for $p \in [1, \infty)$

$$\|x\|_p := \sum_i x_i^p$$

  are **monotone semiring homomorphisms** Major $\to \mathbb{R}_+$.

- The ℓ^∞-norm

$$\|x\|_\infty := \max_i x_i$$

  is a monotone semiring homomorphism Major $\to \mathbb{TR}_+$, where

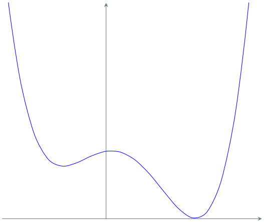
$$\mathbb{TR}_+ := (\mathbb{R}_+, \max, \cdot)$$

  are the **tropical reals**.

- And there are **no other ones**! Morally, this is why the Rényi entropies crop up.

Real algebra(ic geometry)

- When does a polynomial in $f \in \mathbb{R}[X]$ take on only nonnegative values?



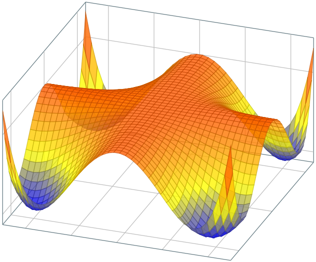
$$f = X^4 - 2X^3 - 6X^2 + 2X + 25$$
$$= (X^2 - X - 4)^2 + (X - 3)^2$$

- Writing f as a sum of squares is a **certificate** of nonnegativity.

- Existence of such a certificate is necessary and sufficient for nonnegativity.

  Proof by fundamental theorem of algebra!

▷ When is $f \in \mathbb{R}[X, Y]$ nonnegative? Example: **Motzkin polynomial**



$$
\begin{aligned}
M &:= X^4Y^2 + X^2Y^4 + 1 - 3X^2Y^2 \\
&= 3\left(\frac{X^4Y^2 + X^2Y^4 + 1}{3} - \sqrt[3]{(X^4Y^2)\cdot(X^2Y^4)\cdot 1}\right) \\
&\geq 0.
\end{aligned}
$$

▷ M *cannot* be written as a sum of squares of polynomials.

▷ M *can* be written as a sum of squares of **rational** functions. Also a certificate of nonnegativity!

Hilbert's 17th problem

Theorem (Artin '27)

Every multivariate polynomial $f \in \mathbb{R}[\underline{X}]$ with $f \geq 0$ can be written as a sum of squares of rational functions:

$$f = \frac{g_1^2 + \ldots + g_m^2}{h^2}$$

for $g_1, \ldots, g_m, h \in \mathbb{R}[\underline{X}]$.

- Surprisingly, no known proof without model theory!

More generally, real algebra studies the relation between:

- geometric positivity:
  taking nonnegative (or positive) values on a set (or spectrum),
- algebraic positivity:
  existence of a nonnegativity (positivity) certificate of a fixed type

A **Positivstellensatz**:

- Gives conditions for when the two coincide (approximately).
- Applies to $\mathbb{R}[\underline{X}]$ or to classes of abstract **ordered rings**.

Real algebra and resource theories

- Traditionally, emphasis on polynomial rings $\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \ldots, X_d]$.

- Resource theories: abstract preordered semirings!

- Most standard applications:

  No algebraic certificate $\implies$ **No geometric inequality**

  Example: Polynomial optimization via semidefinite programming[1], NPA hierarchy.

- Resource-theoretic applications:

  Geometric inequality $\implies$ **Algebraic certificate exists**

[1] Jean Bernard Lasserre. **An introduction to polynomial and semi-algebraic optimization**. Cambridge University Press, Cambridge, 2015.

- I will state a Positivstellensatz for **preordered semirings**, generalizing Strassen's[2].

Definition

An element $u \geq 1$ in a preordered semiring S is **power universal** if for every nonzero $x \in S$ there is $k \in \mathbb{N}$ such that

$$x \leq u^k, \qquad 1 \leq x u^k.$$

- Interpretation: Universal resource which can generate and absorb any other resource object, given enough copies.
- Example: in Major, every x with $|\mathrm{supp}(x)| \geq 2$ and $\|x\|_1 > 1$ is power universal, e.g. $x = (1, 1)$.

[2] Volker Strassen. "The asymptotic spectrum of tensors". In: **J. Reine Angew. Math.** 384 (1988), pp. 102–152.

Theorem (T.F. '19)

S preordered semiring, $u \in S$ power universal.

Let $x, y \in S \setminus \{0\}$. Suppose $f(x) < f(y)$ for all monotone homs

$$f : S \to \mathbb{R}_+ \quad \text{and} \quad f : S \to \mathbb{TR}_+.$$

Then:

(a) There is $a \in S \setminus \{0\}$ such that $ax \leq ay$.

(b) There is k such that

$$u^k x^n \leq u^k y^n \qquad \forall n \gg 1.$$

(c) If y itself is power universal, then

$$x^n \leq y^n \qquad \forall n \gg 1.$$

Conversely: if either of these inequalities holds, then $f(x) \leq f(y)$ for all f.

- ▷ Instead of positivity, the semiring situation is concerned with **comparison**, both geometrically and algebraically.

- ▷ Structure of proof is standard, but the details are intricate. It involves a curious polynomial identity:

$$\sum_{k=0}^{n}\left[a_k\left(\sum_{j=0}^{n} b_j x^{-j}\right)(x+1)\sum_{i=0}^{k-1} x^i + b_k\left(\sum_{j=0}^{n} a_j x^j\right)(x^{-1}+1)\sum_{i=0}^{k-1} x^{-i}\right]$$

$$= \sum_{k=0}^{n}\left[a_k\left(\sum_{j=0}^{n} b_j\right)(x+1)\sum_{i=0}^{k-1} x^i + b_k\left(\sum_{j=0}^{n} a_j\right)(x^{-1}+1)\sum_{i=0}^{k-1} x^{-i}\right].$$

And a reduction to the **semifield** case.

Example

For X compact Hausdorff, $C(X)_{>0} \cup \{0\}$ is a semifield.

Theorem (Preliminary)

For normalized $x, y \in$ Major with $|\mathrm{supp}(x)| \geq 2$, suppose that

$$H_\alpha(x) \geq H_\alpha(y) \qquad \forall \alpha \in [1, \infty)$$

and $H_\infty(x) > H_\infty(y)$.

Then for all $\varepsilon > 0$, there is normalized z such that

$$(1+\varepsilon)\, x \otimes z \ \succ_w \ y \otimes z,$$

and

$$(1+\varepsilon)^n \, x^{\otimes n} \ \succ_w \ y^{\otimes n} \qquad \forall n \gg 1.$$

- ▷ Very similar to existing result[3].

---

[3] Guillaume Aubrun and Ion Nechita. "Catalytic majorization and ℓ_p norms". In: **Comm. Math. Phys.** 278.1 (2008). arXiv:quant-ph/0702153, pp. 133–144.

Theorem (T.F. '19)

For bounded random variables X and Y, suppose that

$$\mathbb{E}[e^{tX}] \leq \mathbb{E}[e^{tY}] \qquad \forall t \geq 0,$$

and $\max X < \max Y$.

Then for all $\varepsilon > 0$ there is bounded Z independent of X and Y such that

$$\mathbf{P}[X + Z \geq c] \leq (1+\varepsilon)\,\mathbf{P}[Y + Z \geq c] \qquad \forall c \in \mathbb{R}.$$

Furthermore, in terms of i.i.d. copies: for all $\varepsilon > 0$,

$$\mathbf{P}\left[\sum_{i=1}^{n} X_i \geq c\right] \leq (1+\varepsilon)^n\,\mathbf{P}\left[\sum_{i=1}^{n} Y_i \geq c\right] \qquad \forall c \in \mathbb{R}, n \gg 1.$$

- Related independent work[4].

---

[4] Xiaosheng Mu et al. **Blackwell dominance in large samples**. arXiv:1906.02838.

Matrix majorization

- P and Q real matrices with n columns. Write: $P(a|x)$.
- $P \succ_w Q$ if there is substochastic R with

$$Q = RP, \qquad \text{i.e.} \quad Q(b|x) = \sum_a R(b|a)\, P(a|x).$$

- Semiring structure is column-wise:

$$(P \oplus Q)(-|x) \; := \; P(-|x) \oplus Q(-|x),$$

$$(P \otimes Q)(-|x) \; := \; P(-|x) \otimes Q(-|x).$$

Matrix majorization

- Now the monotone homomorphisms to $\mathbb{R}_+$ are given by values of the **Hellinger transform**

$$H_\alpha(P) := \sum_a \prod_{x=1}^{n} P(a|x)^{\alpha_x}$$

  parametrized by $\alpha \in \mathbb{R}^n$ with $\alpha_x \geq 0$.

- The Positivstellensatz can be applied, essentially classifying **asymptotic and catalytic matrix majorization**!

- Plenty of quantum information applications (especially for $n = 2$, relative majorization).

Further improvements

- Ultimately we want to get rid of the ε's, obtaining exact conditions for when $x^{\otimes n} \succ y^{\otimes n}$.
- I also have a preliminary result which achieves this (work in progress).
- Concerned with preordered **normed** semirings,

$$\| - \| \; : \; S \to \mathbb{R}_+,$$

  where only elements of equal norm are comparable.
- In Major, this is normalization of probability,

$$\|x\| := \sum_i x_i.$$

Derivations and Shannon entropy

- Then also **order-reversing** homomorphisms are relevant, like

$$x \longmapsto \sum_i x_i^\alpha$$

for $\alpha < 1$.

- And additionally quantities $D : S \to \mathbb{R}_+$ which are additive and satisfy the **Leibniz rule**

$$D(xy) \ = \ \|x\| \, D(y) + D(x) \, \|y\|,$$

making D into a **derivation**.

- What are these latter quantities for Major?

- Additivity implies

$$D((x_1, \ldots, x_n)) = \sum_i \phi(x_i)$$

  for some ϕ.

- The Leibniz rule gives

$$\frac{\phi(pq)}{pq} = \frac{\phi(p)}{p} + \frac{\phi(q)}{q}.$$

- Hence (essentially) get $\phi(p) = -p \log p$, and therefore

$$D(x) = -\sum_i x_i \log x_i.$$