SDP analysis

The Batman, Atul, Tom with the cat

April 11, 2021

Abstract

This note discusses SDP continuity bounds and how they can be used for our analysis.

Contents

1 SDP-valued functions and their continuity

A semidefinite program (SDP) is an optimization problem of the form

$$\begin{aligned} f(A,B) = \text{maximize:} \quad & \langle A, X \rangle \\ \text{subject to:} \quad & \Phi(X) = B \\ & X \geq 0. \end{aligned} \tag{1}$$

linear right?

We call $f(A,B)$ the value of the semidefinite program which is the supremum of $\langle A, X \rangle$ over all X that are feasible ($X \succeq 0$ and $\Phi(X) = B$). In this work we wish to view how the value of an SDP changes as you change A and/or B. Ultimately, we wish to know if the value of an SDP is continuous as a function of A and B. To this end, let us consider the function

$$h(A) = \text{maximize:} \quad \langle A, X \rangle \tag{2}$$

$$\text{subject to:} \quad X \in C \tag{3}$$

where C is a nonempty, convex set. This is a generalization of an~~d~~ SDP which will be convenient for the upcoming analysis. Notice that when C is unbounded, it may be the case that f takes the value $+\infty$. Since we cannot count that high, we use the following definition.

haha...

Definition 1.1. We define the *support* of a function h, denoted as $\text{supp}(h)$, as

$$\text{supp}(h) := \{v : h(v) \text{ is finite}\}. \tag{4}$$

cheating

We now show some elementary properties of this function.

Lemma 1.2. The support of h is convex and h is a convex function on its support.

ooh...

Proof. For $A_1, A_2 \in \text{supp}(h)$ and $\lambda_1, \lambda_2 \geq 0$ satisfying $\lambda_1 + \lambda_2 = 1$, we have

$$\begin{aligned} h(\lambda_1 A_1 + \lambda_2 A_2) &\leq h(\lambda_1 A_1) + h(\lambda_2 A_2) && (5) \\ &= \lambda_1 h(A_1) + \lambda_2 h(A_2) && (6) \\ &< +\infty && (7) \end{aligned}$$

where the last inequality follows from $A_1, A_2 \in \text{supp}(h)$. Thus, $\lambda_1 A_1 + \lambda_2 A_2 \in \text{supp}(h)$, proving $\text{supp}(h)$ is a convex set, and h is convex from the above inequalities. $\square$

The following corollary follows from the fact that h is convex.

Corollary 1.3 ([?])**.** h is continuous on the interior of its support.

Another well-known result is that h is continuous on its entire support if C is compact.

Lemma 1.4. If C is compact, then h has full support and is continuous everywhere.

Proof. If C is compact, then $h(A) = \langle A, X \rangle$ for some $X \in C$ (i.e., X is an optimal solution). Thus, it follows h has full support. Given $A_1, A_2 \in \text{Herm}(\mathcal{X})$, denote by $X_1, X_2 \in C$ the respective optimal solutions such that $h(A_1) = \langle A_1, X_1 \rangle$ and $h(A_2) = \langle A_2, X_2 \rangle$. By symmetry, suppose we have $h(A_1) \geq h(A_2)$. Therefore,

$$\begin{aligned} |h(A_1) - h(A_2)| &= h(A_1) - h(A_2) && (8) \\ &= \langle A_1, X_1 \rangle - \langle A_2, X_2 \rangle && (9) \\ &\leq \langle A_1, X_1 \rangle - \langle A_2, X_1 \rangle && (10) \\ &= \langle A_1 - A_2, X_1 \rangle && (11) \\ &\leq \|A_1 - A_2\|_2 \cdot \|X_1\|_2 && (12) \end{aligned}$$

where we used the optimality of X_1 in the first inequality and Cauchy-Schwarz in the second. Since $X_1 \in C$, which is compact, we know there exists $R > 0$ such that $\|X_1\|_2 \leq R$. Thus, $h(A_1) \to h(A_2)$ as $A_1 \to A_2$, proving h is continuous. $\square$

This may look like it only applies to the case when you change the objective function of an SDP (i.e., the variable A), but it often applies to the case when you change the constant in the constraints as well (i.e., the variable B). This is due to duality theory of semidefinite programming, which we now briefly discuss.

The dual to the SDP (1) is given as

$$\begin{aligned} g(A, B) = \text{minimize:} \quad & \langle B, Y \rangle && (13) \\ \text{subject to:} \quad & \Phi^*(Y) \geq A. && (14) \end{aligned}$$

The utility of this definition is illustrated in the following fact.

Fact 1.5 (Strong duality)**.** Under the assumption that (A, B) satisfies $f(A, B) < +\infty$ and there exists Y such that $\Phi^*(Y) < A$, then we have $f(A, B) = g(A, B)$.

2 Continuity of Alice's SDP (or was it Bob's?

Recall that cheating Alice's SDP has the following form.

$$\begin{aligned} f(A,B) = \text{maximize:} \quad & \langle (0,A),(\rho_1,\rho_2)\rangle && (15)\\ \text{subject to:} \quad & \mathrm{Tr}_M(\rho_2) = \rho_1 \otimes \frac{1}{2}\mathbb{1}_G && (16)\\ & \mathrm{Tr}_S(\rho_1) = B && (17)\\ & \rho_1,\rho_2 \geq 0. && (18)\end{aligned}$$

We now wish to use continuity arguments to prove that solving this SDP (or one like it) provides (or upper bounds) an upper bound on Alice's cheating probability in the limit as self-tests approaches infinity.

From Lemma 1.4 and noting that the feasible region of Alice's cheating SDP is compact, we see that f is continuous in the variable A. We now have to check continuity in the variable B.

The dual of the above SDP is given as **[Jamie: double check]**

$$\begin{aligned} g(A,B) = \text{minimize:} \quad & \langle B, W_0\rangle && (19)\\ \text{subject to:} \quad & W_0 \otimes \mathbb{1}_S \geq \frac{1}{2}\mathrm{Tr}_G(W_1) && (20)\\ & W_1 \otimes \mathbb{1}_M \geq A && (21)\\ & W_1 \geq 0. && (22)\end{aligned}$$

By strong duality (Fact 1.5), we have $f(A,B) = g(A,B)$. Note that the feasible region of the dual is *not* bounded, thus we can only verify continuity on the interior of some set. For this, define **[Jamie: double check]**

$$\begin{aligned} h(B) = \text{maximize:} \quad & \langle B, W_0'\rangle && (23)\\ \text{subject to:} \quad & W_0' \otimes \mathbb{1}_S \leq \frac{1}{2}\mathrm{Tr}_G(W_1') && (24)\\ & W_1' \otimes \mathbb{1}_M \leq -A. && (25)\end{aligned}$$

Note that $h(B) = -g(A,B)$ by associating $(-W_0, -W_1)$ with (W_0', W_1') **[Jamie: double check]**.

We see that for any positive semidefinite matrix B, $h(B)$ is finite (since then $g(A,B)$ is bounded between 0 and $\mathrm{Tr}(B)$), but for B not PSD, $h(B) = +\infty$ (since $g(A,B) = -\infty$ then, due to infeasibility of SDP (15)). Thus,

$$\mathrm{supp}(h) = \{B : B \geq 0\}. \qquad (26)$$

From Lemma 1.3, we have that $h(B)$ is continuous on *positive definite* matrices (being the interior of the set of positive semidefinite matrices). However, the SDPs that we want to solve (in the limit) has B being positive semidefinite and not positive definite. Thus, we need to massage the SDPs a bit to make it work.

Consider the following SDP

$$\begin{aligned} f_\epsilon(A,B) = \text{maximize:} \quad & \langle (0,A),(\rho_1,\rho_2)\rangle && (27)\\ \text{subject to:} \quad & \mathrm{Tr}_M(\rho_2) = \rho_1 \otimes \frac{1}{2}\mathbb{1}_G && (28)\\ & \mathrm{Tr}_S(\rho_1) \leq B + \epsilon\mathbb{1} && (29)\\ & \rho_1,\rho_2 \geq 0 && (30)\end{aligned}$$

noting the added scalar of the identity and the relaxation in the corresponding constraint. (The inequality does not change the value at all, it is just there to illustrate some facts we soon introduce.) From our continuity results concerning the function $f(A, B)$, we can deduce that f_ϵ is continuous for all A and positive *semidefinite* B. **[Jamie: Note to self, check that continuity plays nice with two parameters. I think so, since there is no switching of the two limits.]**

Note that $f_\epsilon(A, B) \geq f(A, B)$ for all $\epsilon > 0$ which can be readily checked. Therefore, for any $\epsilon > 0$ that we fix, there is an $n' > 0$ such that $B_n \leq B + \epsilon \mathbb{1}$ for all $n \geq n'$ where B_n is the density operator coming from the version of the protocol where we use n self-tests **[Jamie: double check]**. Thus, for any ϵ, we have $f_\epsilon(A, B)$ being an upper bound on how much Alice can cheat in the limit of infinite self-tests.

We need to argue that for every n (being the number of self-tests), we get an SDP of the form (15) for some density operator B_n. I will have to look at the formulation again to see if this is the case. But, I have some hope :)