May 5, 2011 SDP in Quantum Information, Ashwin Nayak.

Last time: SDP definition, dual, weak & strong duality, Slater condition, complementary slackness, state-distinguishability as primary example.

Today: Alternative forms of SDPs; Complexity of solving SDPs; QIP, $\oplus$MIP* & non-local games.

Last time, we saw the example of St. Dist., which came with an equality constraint that we converted to a pair of inequalities. We may cut short this additional steps by developing general equivalences ~~with~~ between the form of SDP presented in the last lecture and others with mixed equality & inequality constraints.

A useful alternative form is the following:

Primal (P′)

$$\sup \langle C, X\rangle$$

subject to

$$\Phi_1(X) = B_1$$
$$\Phi_2(X) \leq B_2$$
$$X \geq 0$$

Dual (D′)

$$\inf \langle B_1, Y_1\rangle + \langle B_2, Y_2\rangle$$

subject to

$$\Phi_1^*(Y_1) + \Phi_2^*(Y_2) \geq C$$
$$Y_1 \text{ Hermitian}$$
$$Y_2 \geq 0$$

Here variable $X \in L(H)$

$\Phi_1 : L(H) \to L(K_1)$ is linear (not necessarily Hermitian)

$\Phi_2 : L(H) \to L(K_2)$ — " —

$C \in L(H)$, $B_1 \in L(K_1)$, $B_2 \in L(K_2)$ Hermitian.

$\left.\begin{array}{l}\Phi_1^* : L(K_1) \to L(H) \\ \Phi_2^* : L(K_2) \to L(H)\end{array}\right\}$ adjoints of Φ_1, Φ_2, resp.

(HW : show that this Primal SDP is equivalent to an SDP of form presented earlier, and therefore derive its dual.)

The following gives a more handy condition for strong duality to hold

<u>Theorem</u> : (Slater condition)

(i) If P' is feasible, and D' has a strictly feasible solution (Y_1, Y_2) (i.e. Y_1, Y_2 Hermitian, $Y_2 > 0$, $\Phi_1^*(Y_1) + \Phi_2^*(Y_2) > C$), then strong duality holds & there is a primal feasible X which achieves ~~the~~ optimum.

(ii) If D' is feasible, and P' has a strictly feasible solution X (i.e. $X > 0$ such that $\Phi_1(X) = B_1$, $\Phi_2(X) < B_2$) then, there is a dual feasible Y that achieves the opt (strong duality holds &).

Power of Quantum Interactive Proofs QIP

Consider the following problem:

Quantum Circuit Distinguishability (QCD) (Rosgen, Watrou

Given: two quantum circuits C_1 & C_2 both taking n-qubit inputs & producing m-qubit outputs $(n, m \geq 1)$.

Promise: $\|C_1 - C_2\|_\diamond \geq 3/4$ or $\|C_1 - C_2\|_\diamond \leq 1/4$,

i.e. Either there is a $(2n)$-qubit state $|\psi\rangle$ s.t.

$$\| C_1 \otimes I_n(\psi) - C_2 \otimes I_n(\psi) \|_{tr} \geq 3/4$$

or for all $(2n)$-qubit states $|\psi\rangle$, the above trace distance is $\leq 1/$

Question: Which one of the two cases holds?

Hard problem — In the 1st case, "need" to guess a $(2n)$-qubit state on which C_1 & C_2 differ, and further measure the output states in the optimal manner. Neither is a priori efficiently doable. So possibly not in BQP. However, if we have help from an all-powerful "prover", we may be able to do both.

Protocol

1) Prover: Prepares a $(2n)$-qubit state $|\psi\rangle$ and sends one half of the state (n-qubits) to you (the "verifier").

2) Verifier: Picks a uniformly random one C_i of the circuits C_1 and C_2 and applies C_i to the n qubits received. Sends the m output qubits to the prover.

3) <u>Prover:</u> (Has to guess which C_i was applied)
(tries to identify the state by applying the optimal measurement)
Sends $j \in \{1,2\}$ to verifier

4) <u>Verifier:</u> accepts iff $j = i$.

<u>Claim</u>: The maximum acceptance probability of the verifier is $\frac{1}{2} + \frac{1}{4} \| C_1 - C_2 \|_\diamond$.

(Exercise) No matter what the prover does, when the circuits are far apart, acceptance prob is bounded as above.

So, in the 1st case, prob of acceptance $\geq 11/16$

and in the 2nd case — " — $\leq \frac{9}{16}$

The difference in probs can be driven to exponentially close to 1 by sequential (or parallel) repetition.

This is a typical quantum interactive proof, and decision problems that admit such a proof belong to the complexity class QIP.

How powerful is this model of "computation"?

Celebrated result (LFKN, Shamir) PSPACE $\subseteq$ IP $\subseteq$ classical version of the class QIP), therefore PSPACE $\subseteq$ QIP.

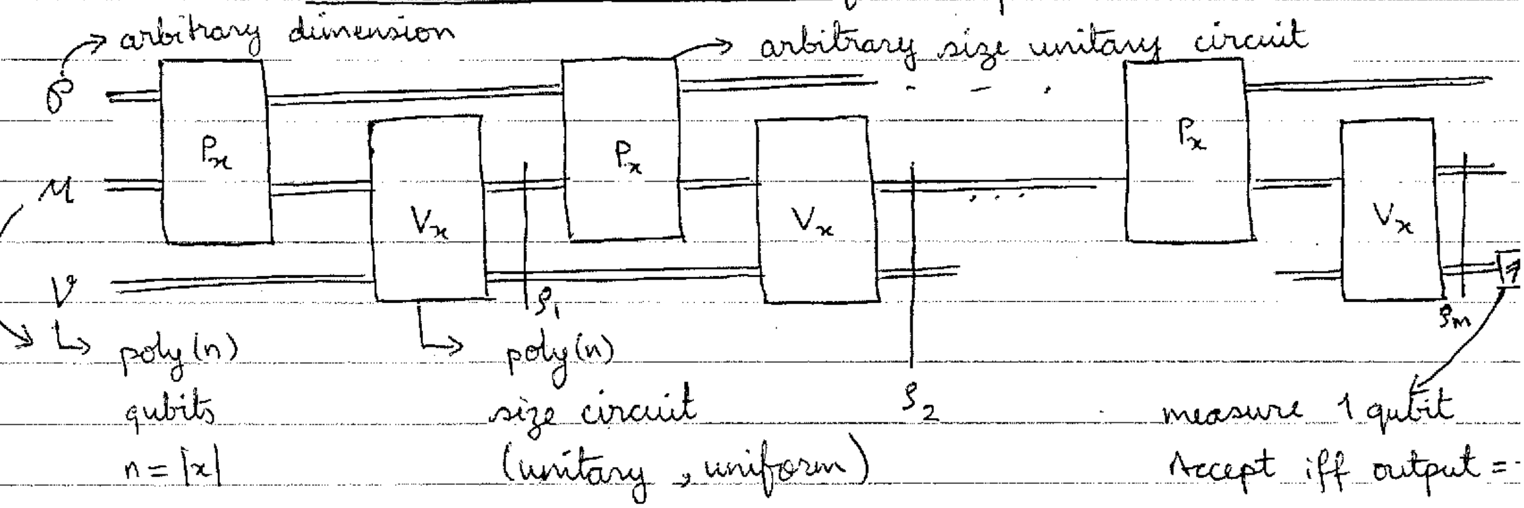
A priori, even with one quantum message **Prover** $\rightarrow$ Verifier, the straightforward classical simulation seems to be in NEXP (guessing the (2^{2n}) dim state in QCD, for example appears to be this hard.)

<u>Today</u> : QIP $\subseteq$ EXP (Kitaev, Watrous)
using SDP.

<u>Note</u> : (1) A stronger result is now known : QIP = PSPACE
(Jain, Ji, Upadhyay, Watrous)
also uses SDP + a parallel SDP solver developed by them

(2) The presentation here is superceded by developments since 2000. (E.g. QCD has been shown to be complete for QIP, and the diamond norm shown to be approximable in P, which implies the above result.) However, the treatment will be used again for another problem.

General <u>Quantum Interactive Proof</u> Input x



All registers start in state $|0\rangle$, w.l.o.g., say we have $m = \mathrm{poly}(n)$ reps of (P_x, V_x)

Let $\Pi_1 = |1\rangle\langle 1| \otimes I$
$\quad\hookrightarrow$ on rest of qubits of $\mathcal{M}$ & $\mathcal{V}$.

$L \in$ QIP iff for any $x \in L$ $\exists P_x$ s.t. acceptance prob $\geq 3/4$ (say)
& if $x \notin L$, $\forall P_x$, acceptance prob $\leq 1/4$.

We can cast the problem of estimating the maximum acceptance probability as an SDP.

Consider the state ρ_i of registers $\mathcal{M}$ & $\mathcal{V}$ after i applications of

$$(I_{\mathcal{P}} \otimes V_x)(P_x \otimes I_{\mathcal{V}}).$$

The SDP: (Primal)

$$\sup \quad \langle I_{\mathcal{P}} \otimes \Pi_1, \rho_m \rangle \qquad \text{(Primal)} \; (P_{QIP})$$

subject to:

$$\mathrm{Tr}_{\mathcal{M}}(V_x^\dagger \rho_1 V_x) = |\bar{0}\rangle\langle\bar{0}|$$

$$\mathrm{Tr}_{\mathcal{M}}(V_x^\dagger \rho_i V_x) = \mathrm{Tr}_{\mathcal{M}}(\rho_{i-1}), \quad i = 2, \ldots, m.$$

$$\rho_1, \rho_2, \ldots, \rho_m \geq 0 \quad \text{in } L(\mathcal{M} \otimes \mathcal{V})$$

(Trace = 1 condition subsumed by 1st constraint.)

Dual SDP:

$$X = \begin{bmatrix} \rho_1 & & & ? \\ & \rho_2 & & \\ & & \ddots & \\ ? & & & \rho_m \end{bmatrix} \qquad \Phi(X) = \begin{bmatrix} \mathrm{Tr}_{\mathcal{M}}(V_x^\dagger \rho_1 V_x) & & \Theta \\ & \mathrm{Tr}_{\mathcal{M}}(V_x^\dagger \rho_2 V_x) - \mathrm{Tr}_{\mathcal{M}}(\rho_1) & \\ \Theta & & \ddots \end{bmatrix}$$

$$X \in L\left(\bigoplus^m (\mathcal{M} \otimes \mathcal{V})\right) \qquad \Phi(X) \in L\left(\bigoplus^m \mathcal{V}\right).$$

$$Y = \begin{bmatrix} Y_1 & & ? \\ & \ddots & \\ ? & & Y_m \end{bmatrix} \qquad \Phi^*(Y) = \begin{bmatrix} V_x(I_{\mathcal{M}} \otimes Y_1)V_x^\dagger - I_{\mathcal{M}} \otimes Y_2 & & \Theta \\ & V_x(I_{\mathcal{M}} \otimes Y_2)V_x^\dagger - I_{\mathcal{M}} \otimes Y_3 & \\ \Theta & & \ddots \\ & & & V_x(I_{\mathcal{M}} \otimes Y_m)V_x^\dagger \end{bmatrix}$$

(HW exercise: derive the adjoint Φ^* above)

$$C = \begin{bmatrix} 0 & & & 0 \\ & 0 & & \\ & & 0 & \\ 0 & & & \ddots \\ & & & & I_M \otimes \Pi_1 \end{bmatrix} \qquad B = \begin{bmatrix} |\bar{0}\rangle\langle\bar{0}| & & 0 \\ & 0 & \\ 0 & & \ddots \\ & & & 0 \end{bmatrix}$$

So, the dual problem is (using the alternative form of SDP above):

$$\inf \quad \langle |\bar{0}\rangle\langle\bar{0}|, Y_1 \rangle \qquad\qquad (D_{QIP})$$

subject to:

$$V_x (I_M \otimes Y_i) V_x^{+} \geq I_M \otimes Y_{i+1} \qquad \forall\ i = 1, \ldots, m-1$$

$$V_x (I_M \otimes Y_m) V_x^{+} \geq I_M \otimes \Pi_1$$

$Y_1, \ldots, Y_m$ are Hermitian

(last condition is redundant; the last inequality implies Y_m is P.S.D., so all Y_i are P.S.D.)

<u>Claim</u> Every primal feasible solution corresponds to a valid prover strategy (i.e. there is a space $\mathcal{P}$, and a unitary P_x such that the intermediate reduced states in the protocol are $S_1, \ldots, S_m$).

(Exercise) The other direction is straightforward — holds by construction

<u>Claim</u> The primal is feasible, and the dual is strictly feasible:

The sequence of states obtained by taking $P_x = \frac{I_M \otimes \mathcal{V}}{\dim(M \otimes \mathcal{V})}$ gives us a primal feasible solution.

We get a strictly feasible dual solution by setting

$$Y_m = 2 I_{\mathcal{V}}$$

$$Y_{m-j} = (2+j)\, I_{\mathcal{V}}, \quad j = 0, 1, \ldots, m-1.$$

So strong duality holds, and, as can be deduced independently as well, the primal has a feasible optimum solution.

This SDP formulation helps us solve a problem in the complexity class QIP in EXP: the description of the operators (Φ, C, B) requires us to specify exp(poly(n)) matrix coefficients, each of which may be represented with polynomially many bits.
Further, under suitable conditions, SDPs may be approximated efficiently.

Say $R, r \in \mathbb{R}^{>0}$.

<u>Definition</u>: We say a (convex) set K is well-bounded with parameters (R, r), if there are Euclidean balls of radii R & r, say $S(x,R)$ & $S(y,r)$, respectively (centred at x & y) s.t. $S(x,R)$ contains the set K and $S(y,r)$ is contained in K:

$$S(y,r) \subseteq K \subseteq S(x,R)$$

$$\Phi = (\Phi_1, \Phi_2), \quad B = (B_1, B_2)$$

<u>Theorem</u> Given (Φ, C, B), λ, $B_i \in L(\mathcal{K}_i)$, $C \in L(\mathcal{H})$, $\dim(\mathcal{H}) = N$, $\dim(\mathcal{K}_i) = M_i$, $\Phi_i : L(\mathcal{H}) \to L(\mathcal{K}_i)$; as the specification of an SDP; a parameter $\varepsilon > 0$.

If either the (primal or dual) feasible region is well-bounded with parameters (R, r), then the (corresponding primal / dual) SDP is efficiently approximable — ie, there is an algorithm that runs in time polynomial in $\log(R/r)$, $\log\frac{1}{\varepsilon}$, $\dim(\mathcal{H})$, $\dim(\mathcal{K}_i)$, & the max bit length of matrix coefficients λ, and produces a feasible solution at which the objective function value is within ε of the optimum.

For the SDP that captures the maximum acceptance probability of a quantum interactive proof, the well-boundedness condition is easier to verify for the dual (DQIP). First, the optimum doesn't change if we add constraints $Y_i \leq 2 I_{\mathcal{V}}$, say. Then, the feasible region $\subseteq S(0,R)$, where $R = 2 \dim(\mathcal{V})$, and it contains a ball of radius $1/2m$ around a dual feasible point (HW: find such a point).

Thus, given an input to a language $L \in QIP$, we may determine in EXP, whether the maximum acceptance probability $\geq 3/4$ or $\leq 1/4$ (by choosing the precision parameter ε to be, say, $1/8$).

— Such an approach to bounding the power of quantum computational models using SDP was also used by Cleve, Hoyer, Toner, & Watrous to show that $\oplus MIP^* \subseteq EXP$, whereas $\oplus MIP = NEXP$ — if the two provers in a multi-prover one-round classical interactive proof share quantum entangle-ment, the verifier's power is considerably reduced.

— The SDP characterization in the above result was also used by Cleve, Slofstra, Unger, Upadhyay to show that quantum XOR-non-local games satisfy the perfect strong direct product property/ perfect parallel repetition theorem.

(next module)

— The general approach of casting quantum strategies as convex optimization problems has also been pursued by Kitaev and Mochon for coin-flipping, and by Gutoski and Watrous for refereed games. (Also by Gutoski & Wu.)