

Semidefinite programming hierarchies for quantum-assisted coding

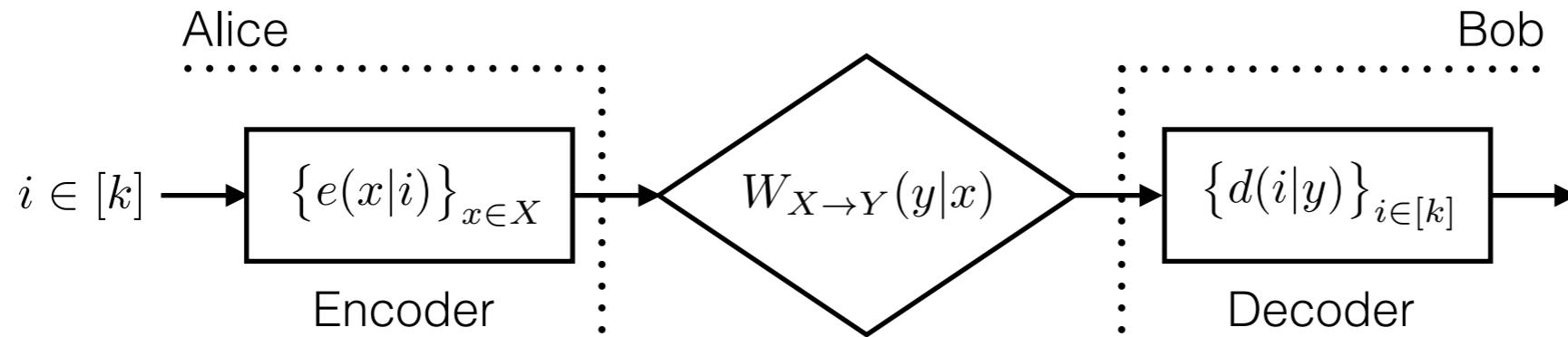
Mario Berta, Omar Fawzi, Volkher Scholz

based on

SIAM Journal on Optimization 26 (3), 1529 (2016)

August 13th, 2018, Modern Topics in Quantum Information, Natal Brazil

Noisy channel coding



- Given noisy channel $W_{X \rightarrow Y}$ mapping X to Y with transition probability:
$$W_{X \rightarrow Y}(y|x) \quad \forall (x, y) \in X \times Y$$
- The goal is to send k different messages using W while minimizing the error probability for decoding:

$$p_{\text{succ}}(W, k) := \underset{(e,d)}{\text{maximize}} \quad \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x)e(x|i)d(i|y) \quad \text{"bilinear optimisation"}$$

subject to

$$\sum_x e(x|i) = 1 \quad \forall i \in [k], \quad \sum_i d(i|y) = 1 \quad \forall y \in Y$$

$$0 \leq e(x|i) \leq 1 \quad \forall (x, i) \in X \times [k], \quad 0 \leq d(i|y) \leq 1 \quad \forall (i, y) \in [k] \times Y.$$

Noisy channel coding

$$p_{\text{succ}}(W, k) := \underset{(e,d)}{\text{maximize}} \quad \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) e(x|i) d(i|y)$$



subject to $\sum_x e(x|i) = 1 \quad \forall i \in [k], \quad \sum_i d(i|y) = 1 \quad \forall y \in Y$

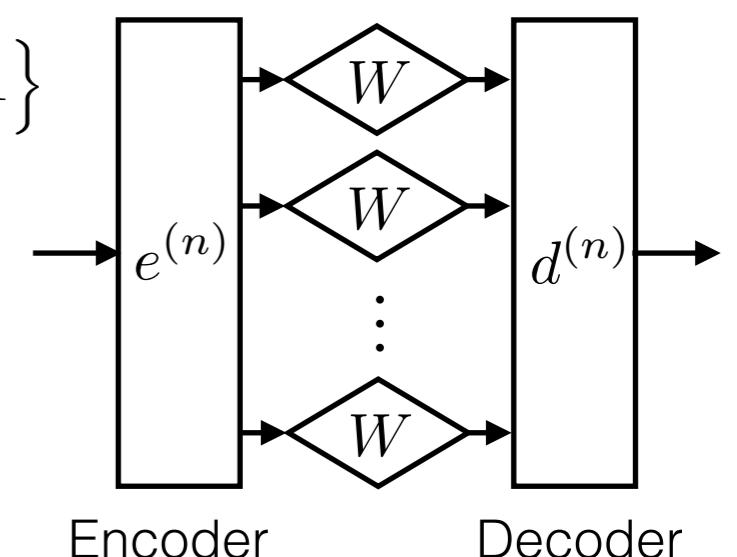
$$0 \leq e(x|i) \leq 1 \quad \forall (x, i) \in X \times [k], \quad 0 \leq d(i|y) \leq 1 \quad \forall (i, y) \in [k] \times Y.$$

compared to

- Shannon's asymptotic independent and identical distributed (iid) channel capacity:

Definition: $C(W) := \sup \left\{ R \mid \forall \delta > 0 : \lim_{n \rightarrow \infty} p_{\text{succ}}(W^{\times n}, [R(1 - \delta)]^n) = 1 \right\}$

Answer: $C(W) = \max_{P_X} I(X : Y)$ mutual information



Noisy channel coding

$$p_{\text{succ}}(W, k) := \underset{(e,d)}{\text{maximize}} \quad \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) e(x|i) d(i|y)$$

subject to $\sum_x e(x|i) = 1 \quad \forall i \in [k], \quad \sum_i d(i|y) = 1 \quad \forall y \in Y$

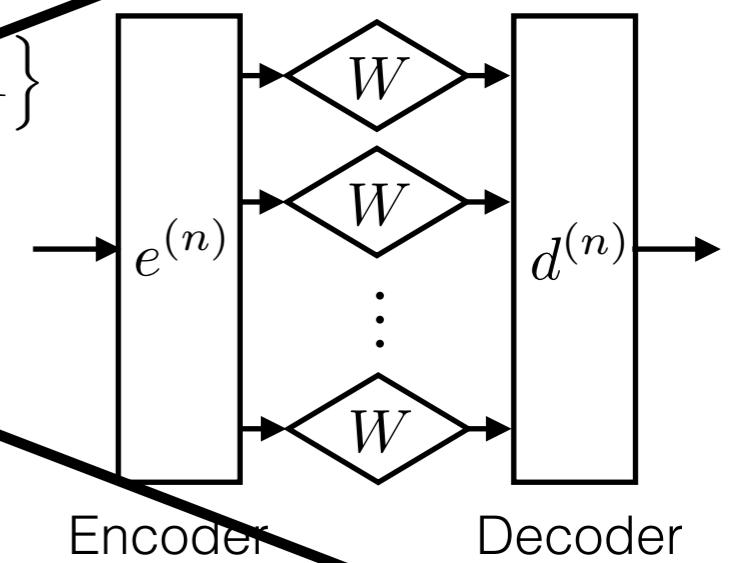
$$0 \leq e(x|i) \leq 1 \quad \forall (x,i) \in X \times [k], \quad 0 \leq d(i|y) \leq 1 \quad \forall (i,y) \in [k] \times Y.$$

compared to

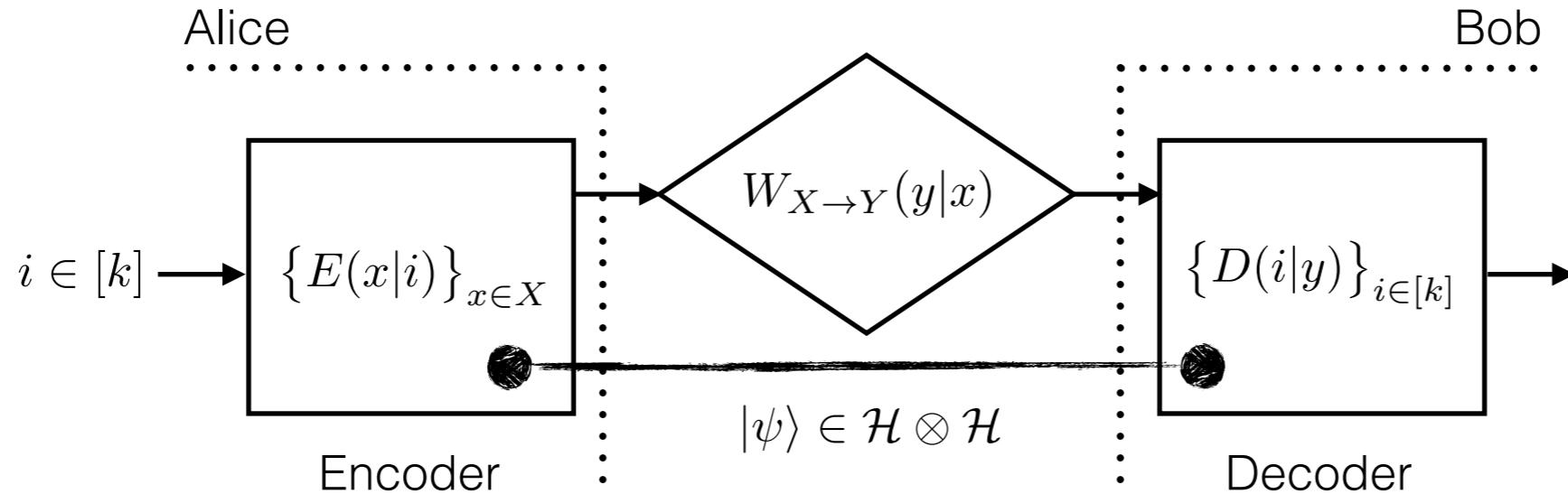
- Shannon's asymptotic independent and identical distributed (iid) channel capacity:

Definition: $C(W) := \sup \left\{ R \mid \forall \delta > 0 : \lim_{n \rightarrow \infty} p_{\text{succ}}(W^{\times n}, [R(1 - \delta)]^n) = 1 \right\}$

Answer: $C(W) = \max_{P_X} I(X : Y)$ mutual information



Quantum-assisted channel coding



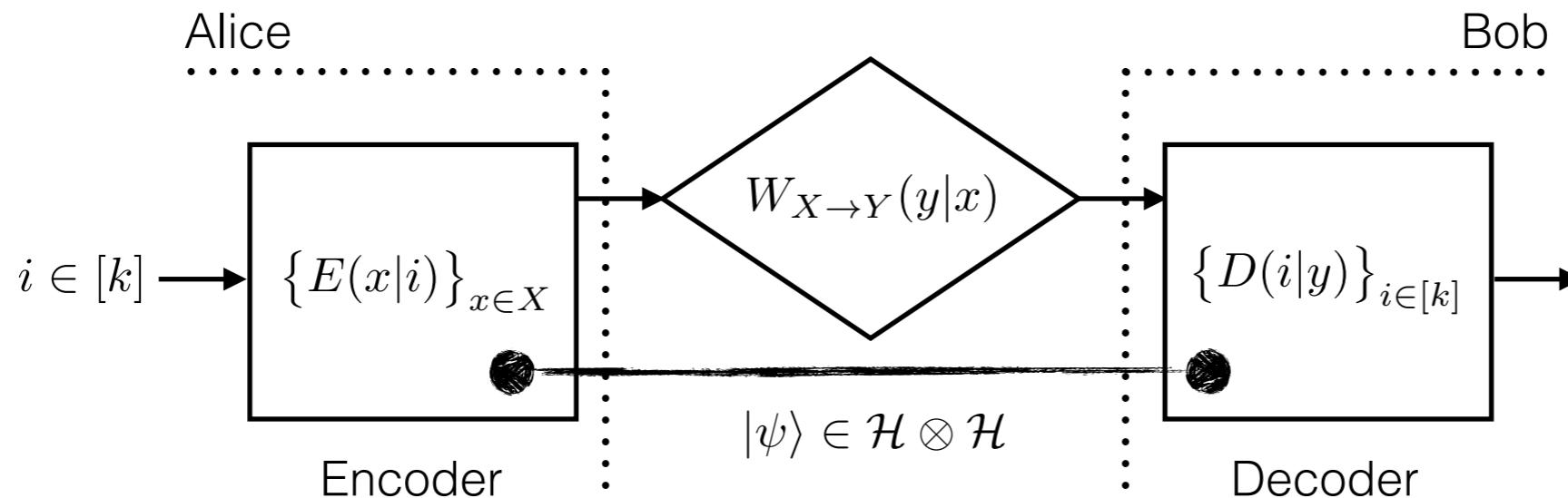
$$p_{\text{succ}}^*(W, k) := \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} \quad \frac{1}{k} \sum_{x, y, i} W_{X \rightarrow Y}(y|x) \langle \psi | E(x|i) \otimes D(i|y) | \psi \rangle \quad \text{"quantum bilinear optimisation"}$$

subject to

$$\sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k], \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$$

$$0 \leq E(x|i) \leq 1_{\mathcal{H}} \quad \forall (x, i) \in X \times [k], \quad 0 \leq D(i|y) \leq 1_{\mathcal{H}} \quad \forall (i, y) \in [k] \times Y.$$

Quantum-assisted channel coding



$$p_{\text{succ}}^*(W, k) := \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} \quad \frac{1}{k} \sum_{x, y, i} W_{X \rightarrow Y}(y|x) \langle \psi | E(x|i) \otimes D(i|y) | \psi \rangle \quad \text{"quantum bilinear optimisation"}$$

subject to $\sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k], \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y$

$0 \leq E(x|i) \leq 1_{\mathcal{H}} \quad \forall (x, i) \in X \times [k], \quad 0 \leq D(i|y) \leq 1_{\mathcal{H}} \quad \forall (i, y) \in [k] \times Y.$

- **Scalar** (commutative) versus **matrix** (non-commutative) variables:

$$p_{\text{succ}}(W, k) := \underset{(e, d)}{\text{maximize}} \quad \frac{1}{k} \sum_{x, y, i} W_{X \rightarrow Y}(y|x) e(x|i) d(i|y)$$

- Unknown if $p_{\text{succ}}^*(W, k)$ is computable

Quantum-assisted channel coding

- Understand the possible separation: $p_{\text{succ}}(W, k)$ versus $p_{\text{succ}}^*(W, k)$

- For the asymptotic iid capacity quantum assistance does not help:

$$C(W) = C^*(W) \quad [\text{Bennett et al., PRL (1999)}]$$

- In general, there is a **separation**:

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

$$p_{\text{succ}}(Z, 2) = \frac{5}{6} \approx 0.833 \quad \text{vs.} \quad p_{\text{succ}}^*(Z, 2) \geq \frac{2 + 2^{-1/2}}{3} \approx 0.902$$

[Prevedel et al., PRL (2011)]

—> this is also optimal with two-dimensional assistance

[Hemenway et al., PRA (2013)]

[Williams and Bourdon, arXiv:1109.1029]

- However, $[0.902, 1] \ni p_{\text{succ}}^*(Z, 2) = ?$

- We give a **converging hierarchy of semidefinite programming (sdp) relaxations**:

$$p_{\text{succ}}(W, k) \leq p_{\text{succ}}^*(W, k) = \text{sdp}_\infty(W, k) \leq \dots \leq \text{sdp}_1(W, k)$$

First level sdp relaxation

- Quantum bilinear program:

$$\begin{aligned} p_{\text{succ}}^*(W, k) := \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} \quad & \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x)\langle\psi|E(x|i) \otimes D(i|y)|\psi\rangle \\ \text{subject to} \quad & \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k], \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y \\ & 0 \leq E(x|i) \leq 1_{\mathcal{H}} \quad \forall (x, i) \in X \times [k], \quad 0 \leq D(i|y) \leq 1_{\mathcal{H}} \quad \forall (i, y) \in [k] \times Y. \end{aligned}$$

First level sdp relaxation

- Quantum bilinear program:

idea: relaxation of this bilinear form

$$\begin{aligned}
 p_{\text{succ}}^*(W, k) := & \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} \quad \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) \langle \psi | E(x|i) \otimes D(i|y) | \psi \rangle \\
 & \text{subject to} \quad \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k], \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y \\
 & \quad 0 \leq E(x|i) \leq 1_{\mathcal{H}} \quad \forall (x, i) \in X \times [k], \quad 0 \leq D(i|y) \leq 1_{\mathcal{H}} \quad \forall (i, y) \in [k] \times Y.
 \end{aligned}$$

- First step: see  as the part of the upper-right block of the Gram matrix

$$\Omega = \sum_{u,v} \langle \psi | X_u X_v | \psi \rangle |u\rangle \langle v| \quad \text{with} \quad X_u = \begin{cases} E(x|i) & u = (i, x) \\ D(j|y) & u = (j, y) \end{cases}$$

$$\Omega = \begin{pmatrix} \langle \psi | E(x|i) \cdot E(x'|i') | \psi \rangle & \langle \psi | E(x|i) \cdot D(y|j) | \psi \rangle \\ \langle \psi | E(x'|i') \cdot D(y'|j') | \psi \rangle & \langle \psi | D(y|j) \cdot D(y'|j') | \psi \rangle \end{pmatrix}^{\text{for } i=j}$$

- Original constraints can be formulated as positivity conditions on Ω : $\text{sdp}_1(W, k)$

*motivated by: “**NPA hierarchy**” (for polynomial optimization, study of Bell inequalities)*

[Lasserre, SIAM (2001)], [Parrilo, Math. Program. (2003)], [Navascues et al., PRL (2007)],
 [Doherty et al., IEEE CCC (2008)], [Navascues et al., NJP (2008)], [Pironio et al., SIAM (2010)]

First level sdp relaxation

- First level relaxation: $p_{\text{succ}}(W, k) \leq p_{\text{succ}}^*(W, k) \leq \text{sdp}_1(W, k)$

$$\begin{aligned} \text{sdp}_1(W, k) = \underset{\Omega}{\text{maximize}} \quad & \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) \Omega_{(i,x),(i,y)} \\ \text{subject to} \quad & \Omega \in \text{Pos}(1 + k|X| + k|Y|), \quad \Omega_{\emptyset,\emptyset} = 1 \quad \text{with } \emptyset \text{ the empty symbol} \\ & \Omega_{u,v} \geq 0 \quad \forall u, v \in X \times [k] \cup Y \times [k] \cup \{\emptyset\} \\ & \sum_x \Omega_{w,(i,x)} = \Omega_{w,\emptyset} \quad \forall i \in [k], w \in X \times [k] \cup Y \times [k] \cup \{\emptyset\} \\ & \sum_i \Omega_{w,(i,y)} = \Omega_{w,\emptyset} \quad \forall y \in Y, w \in X \times [k] \cup Y \times [k] \cup \{\emptyset\}. \end{aligned}$$

First level sdp relaxation

- First level relaxation: $p_{\text{succ}}(W, k) \leq p_{\text{succ}}^*(W, k) \leq \text{sdp}_1(W, k) \leq \text{lp}_1(W, k) \leq \text{const} \cdot p_{\text{succ}}(W, k)$

$$\text{sdp}_1(W, k) = \underset{\Omega}{\text{maximize}} \quad \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) \Omega_{(i,x),(i,y)}$$

[Barman and Fawzi, Proc. IEEE ISIT (2016)]

subject to $\Omega \in \text{Pos}(1 + k|X| + k|Y|), \quad \Omega_{\emptyset, \emptyset} = 1$ with \emptyset the empty symbol

new condition $\rightarrow \Omega_{u,v} \geq 0 \quad \forall u, v \in X \times [k] \cup Y \times [k] \cup \{\emptyset\}$

$$\begin{aligned} \sum_x \Omega_{w,(i,x)} &= \Omega_{w,\emptyset} \quad \forall i \in [k], w \in X \times [k] \cup Y \times [k] \cup \{\emptyset\} \\ \sum_i \Omega_{w,(i,y)} &= \Omega_{w,\emptyset} \quad \forall y \in Y, w \in X \times [k] \cup Y \times [k] \cup \{\emptyset\}. \end{aligned}$$

- Going back to our example:

$$Z = \begin{pmatrix} 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/3 \\ 0 & 1/3 & 1/3 & 0 \end{pmatrix}$$

(NPA first level and non-signalling bounds are one)

$$p_{\text{succ}}(Z, 2) = \frac{5}{6} \approx 0.833$$

$$p_{\text{succ}}^*(Z, 2) \geq \frac{2 + 2^{-1/2}}{3} \approx 0.902$$

(known before, with two-dimensional assistance)

- Relaxation: $p_{\text{succ}}^*(Z, 2) \leq \text{sdp}_1(Z, 2) \approx 0.908 = \frac{1}{2} + \frac{1}{\sqrt{6}}$
- Four-dimensional assistance: $p_{\text{succ}}^*(Z, 2) \geq \frac{1}{2} + \frac{1}{\sqrt{6}}$

Quantum bilinear optimization

- Quantum-assisted channel coding:

$$\begin{aligned}
 p_{\text{succ}}^*(W, k) := & \underset{(\mathcal{H}, \psi, E, D)}{\text{maximize}} \quad \frac{1}{k} \sum_{x,y,i} W_{X \rightarrow Y}(y|x) \langle \psi | E(x|i) \otimes D(i|y) | \psi \rangle \\
 \text{subject to} \quad & \sum_x E(x|i) = 1_{\mathcal{H}} \quad \forall i \in [k], \quad \sum_i D(i|y) = 1_{\mathcal{H}} \quad \forall y \in Y \\
 & 0 \leq E(x|i) \leq 1_{\mathcal{H}} \quad \forall (x, i) \in X \times [k], \quad 0 \leq D(i|y) \leq 1_{\mathcal{H}} \quad \forall (i, y) \in [k] \times Y.
 \end{aligned}$$

- General form:

$$\begin{aligned}
 p^*[A, \mathcal{G}, \mathcal{K}] := & \underset{(\mathcal{H}, \psi, E_\alpha, D_\beta)}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \langle \psi | E_\alpha D_\beta | \psi \rangle \\
 \text{subject to} \quad & [E_\alpha, D_\beta] = 0 \quad \forall (\alpha, \beta) \in [N] \times [M] \\
 & g(E_1, \dots, E_N) \geq 0 \quad \forall g \in \mathcal{G} \\
 & k(D_1, \dots, D_M) \geq 0 \quad \forall k \in \mathcal{K}.
 \end{aligned}$$

where: (i) Hilbert space \mathcal{H} with $\psi \in \mathcal{H}$, $\|\psi\| = 1$

- (ii) Hermitian bounded operators $E_\alpha, D_\beta \in \mathcal{B}(\mathcal{H})$
- (iii) sets of affine constraints $\mathcal{G} := \{g(z_1, \dots, z_N)\}$ and $\mathcal{K} := \{k(y_1, \dots, y_M)\}$

Quantum bilinear optimization

$$\begin{aligned}
 \text{sdp}_1[A, \mathcal{G}, \mathcal{K}] = & \underset{\Omega^1}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \Omega_{(\alpha), (\beta)}^1 \\
 \text{subject to} \quad & \Omega^1 \in \text{Pos}(1 + N + M) \\
 & \Omega_{\emptyset, \emptyset}^1 = 1 \\
 & \sum_{i, j=0}^{N+M} f^i \bar{f}^j \Omega_{(i), (j)}^1 \geq 0 \quad \forall f, \bar{f} \in \mathcal{G} \cup \mathcal{K} \cup \{f_z := 1\} .
 \end{aligned}$$

$g^i \bar{g}^j$ and $k^i \bar{k}^j$
*conditions different from
NPA hierarchy*

- First level sdp of NPA hierarchy:

$$\begin{aligned}
 \tilde{\text{sdp}}_1[A, \mathcal{G}, \mathcal{K}] = & \underset{\tilde{\Omega}^1}{\text{maximize}} \quad \sum_{\alpha, \beta} A_{\alpha, \beta} \tilde{\Omega}_{(\alpha), (\beta)}^1 \\
 \text{subject to} \quad & \tilde{\Omega}^1 \in \text{Pos}(1 + N + M) \\
 & \tilde{\Omega}_{\emptyset, \emptyset}^1 = 1 \\
 & \sum_{i=0}^{N+M} f^i \tilde{\Omega}_{(i), \emptyset}^1 \geq 0 \quad \forall f \in \mathcal{G} \cup \mathcal{K} \cup \{f_z := 1\} .
 \end{aligned}$$

$g^i \bar{k}^j$
*conditions from higher
levels in NPA hierarchy*

Quantum bilinear optimization

- Central idea: considering higher order products of the variables X_u leads to more positivity constraints
- Second level $\text{sdp}_2[A, \mathcal{G}, \mathcal{K}]$ from positive constraints on the larger matrix:

$$\Omega^2 = \sum_{u_1 u_2 v_1 v_2} \text{tr} [(X_{u_1} X_{v_1})^* X_{u_2} X_{v_2}] |u_1 u_2\rangle\langle v_1 v_2| \quad \text{with} \quad X_u = \begin{cases} E_\alpha & u = \alpha \\ D_\beta & u = \beta \end{cases}$$

Asymptotically **convergent sdp hierarchy**

$$p^*(A, \mathcal{G}, \mathcal{K}) = \lim_{n \rightarrow \infty} \text{sdp}_n(A, \mathcal{G}, \mathcal{K})$$

- Additional constraints compared to NPA hierarchy important for some applications and lead to natural properties of the sdp relaxations (analytically / numerically)

Conclusion

- (Improved) sdp outer hierarchy for bounding quantum advantage:
 - (i) Quantum-assisted **channel coding**
 - (ii) Quantum value of **two-prover games**
 - > first level in independent work [Sikora and Varvitsiotis, Math. Program. (2016)]
 - (iii) Upper bound the power of **quantum adversaries** in cryptography
 - > cf. [B. et al., IEEE Trans. on Information Theory (2017)]
 - (iv) Outer hierarchy for **completely positive semi-definite cone**: quantum graph parameters, zero-error quantum information theory, etc.
 - > see [Laurent and Piovesan, SIAM Journal on Optimization (2015)]
- Fully quantum problems? Omar this morning.