ICTQT/IFTiA/KCIK Seminar

April 10, 2020

Playing Games with Multiple Access Channels

Nature Communications **11**, 1497 (2020)

arXiv:1909.02479

Felix Leditzky

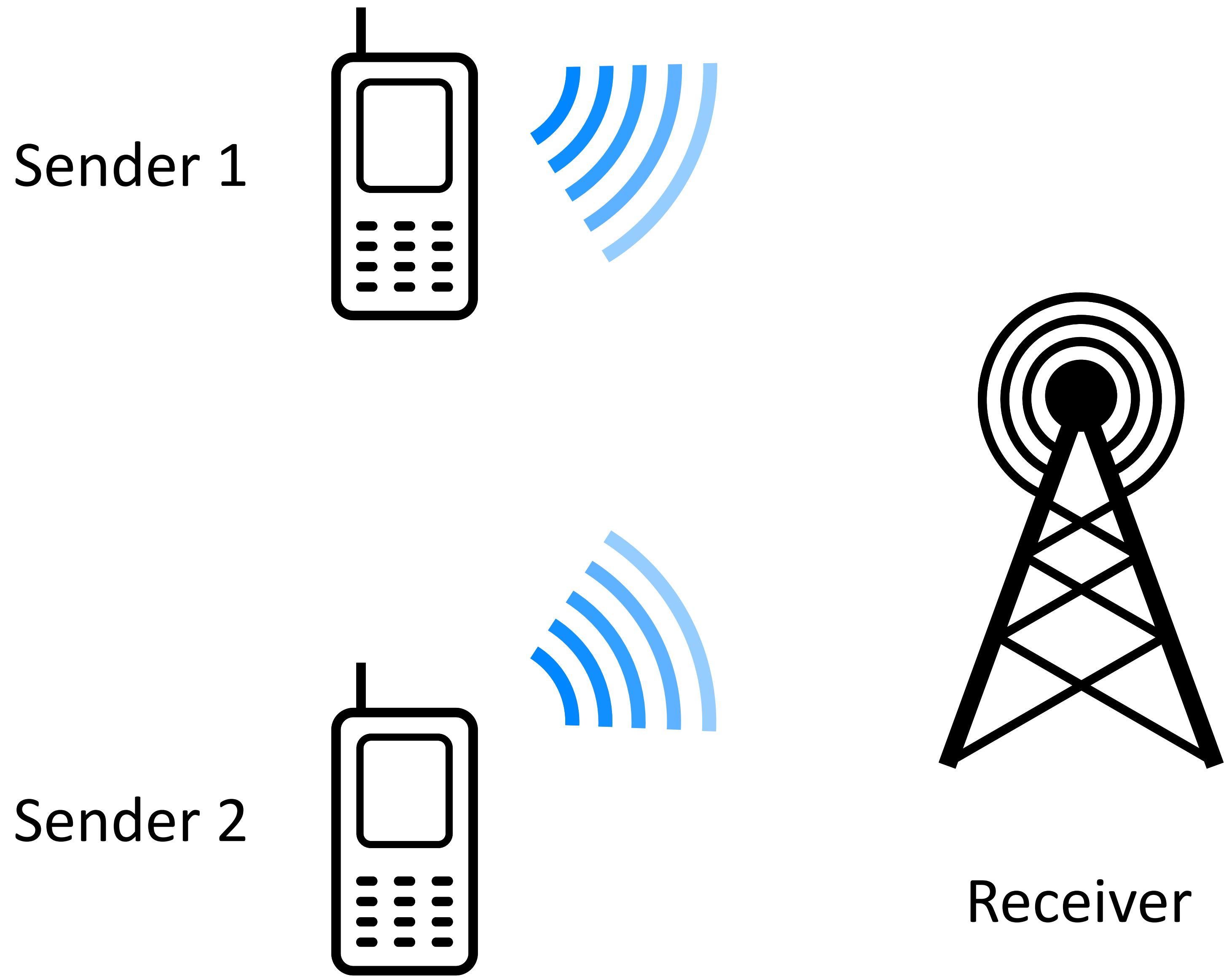
IQC, University of Waterloo

Perimeter Institute

Joint work with Mohammad Alhejji, Joshua Levin, Graeme Smith (CU Boulder)

Multiple access channel

Simplest network communication scenario involving two senders and one receiver.



Goal

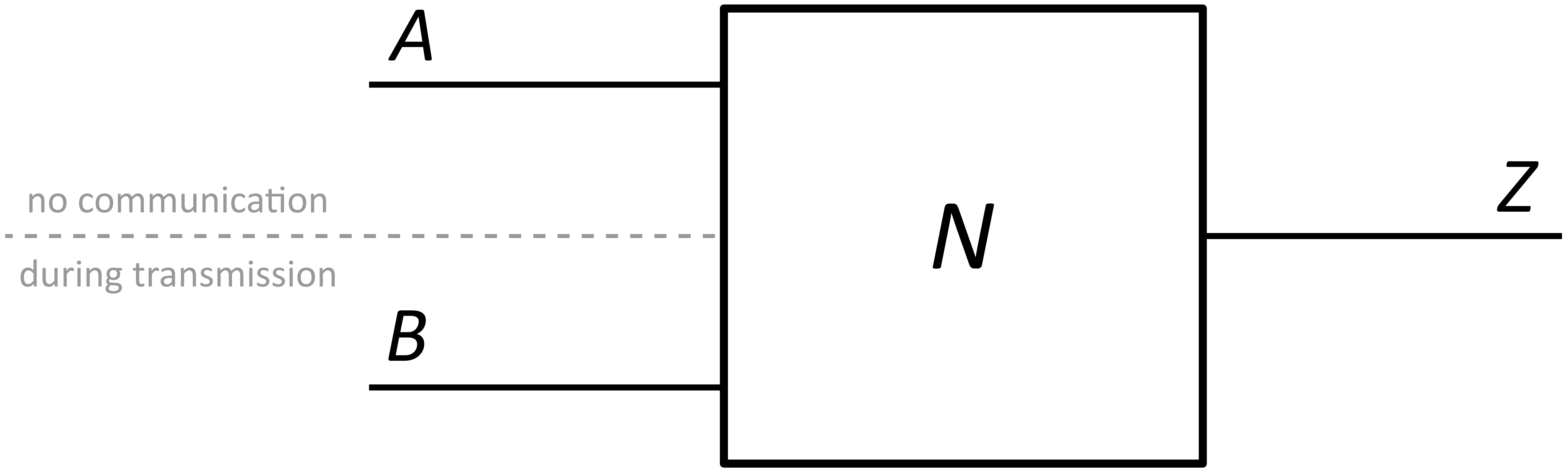
Each sender transmits individual classical messages through common channel to the receiver.

Multiple access channel

MAC: conditional probability distribution $N(z|a, b)$.

Random variables: $(A, B) \xrightarrow{N} Z$

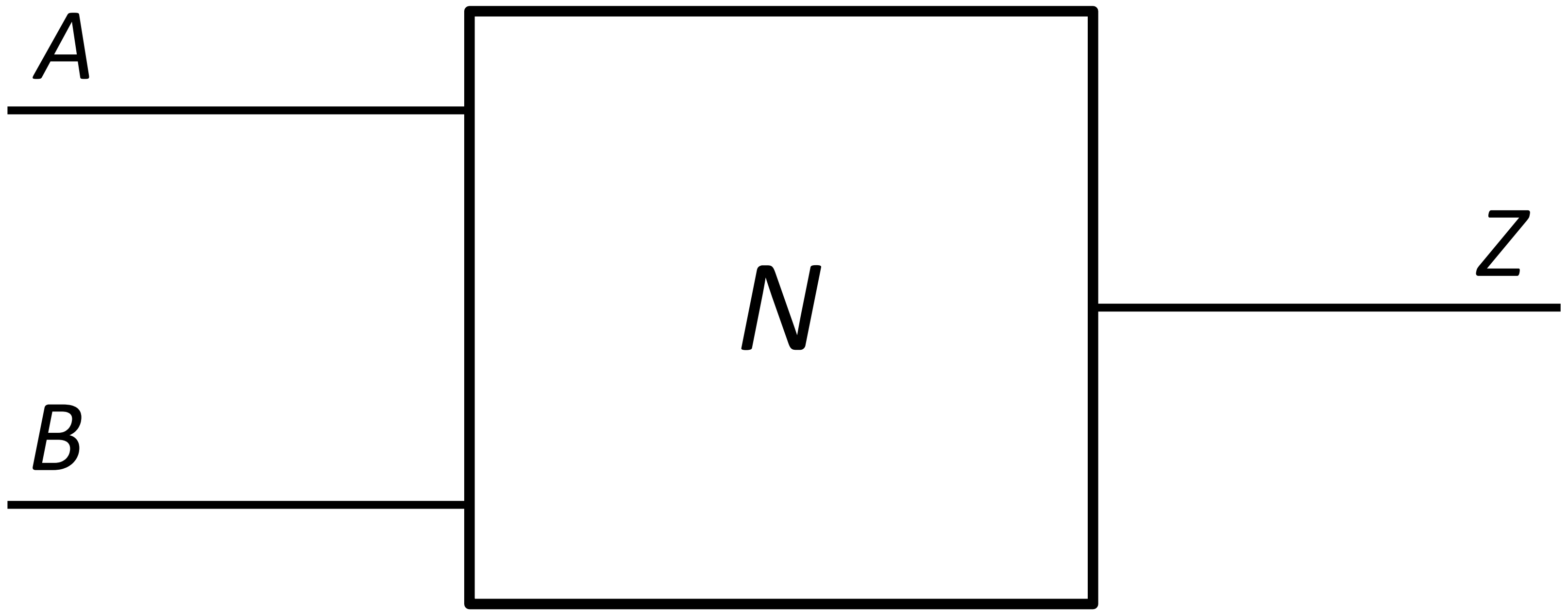
No communication between senders: input RVs A, B are **independent**.



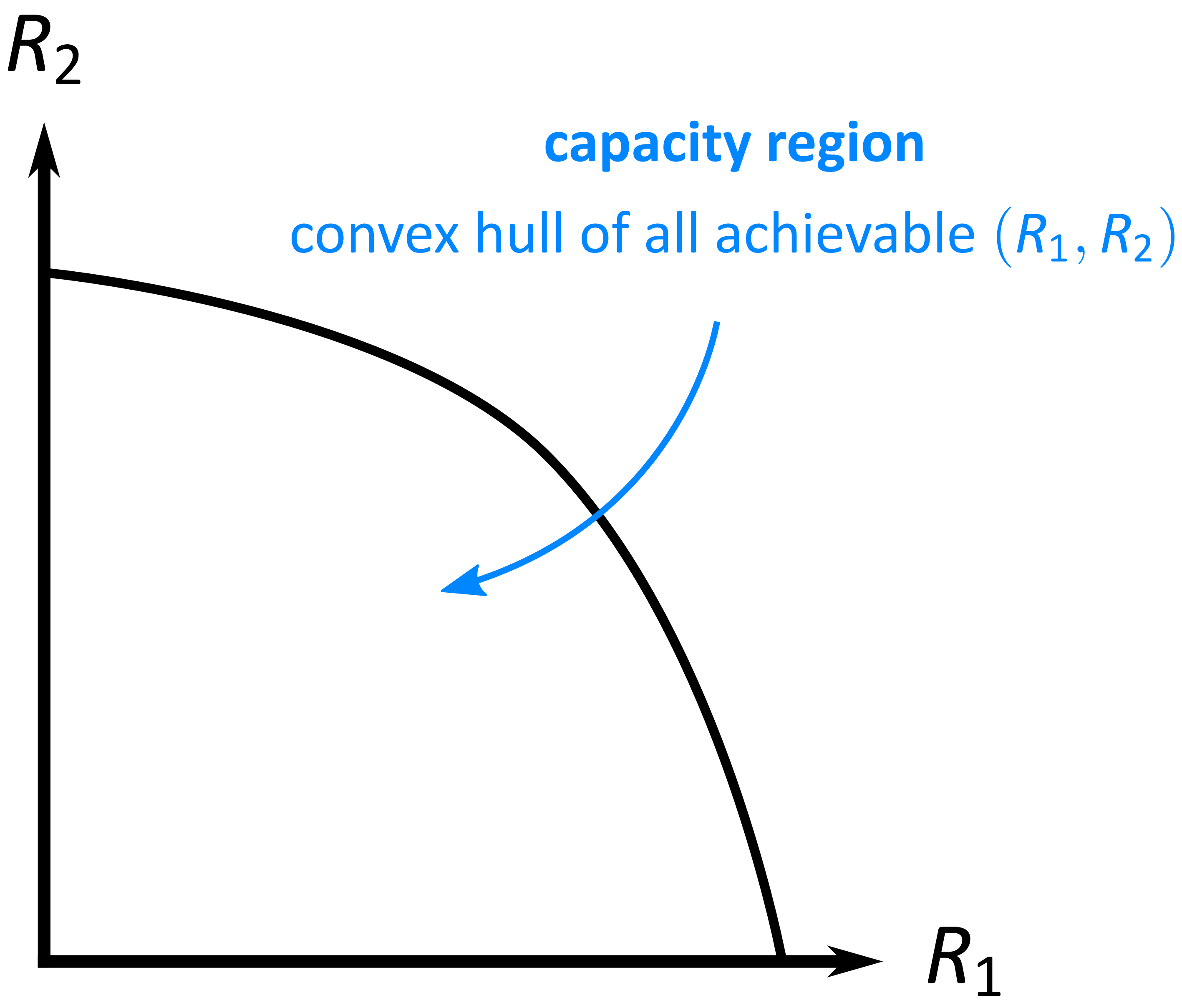
Capacity region of a MAC

Sender 1 (2) tries to send information at rate R_1 (R_2).

(R_1, R_2) is called *achievable* if receiver can decode the two messages with vanishing error.



Multiple access channel



Typical capacity region

Locality & quantum correlations

The independence constraint for the two senders in the MAC scenario can be interpreted as a locality constraint.

Bell inequalities: quantum correlations are strict superset of classical correlations.

Central questions in our work

Can entanglement assistance increase the capacity region of a MAC?

YES (and it can be complicated...)

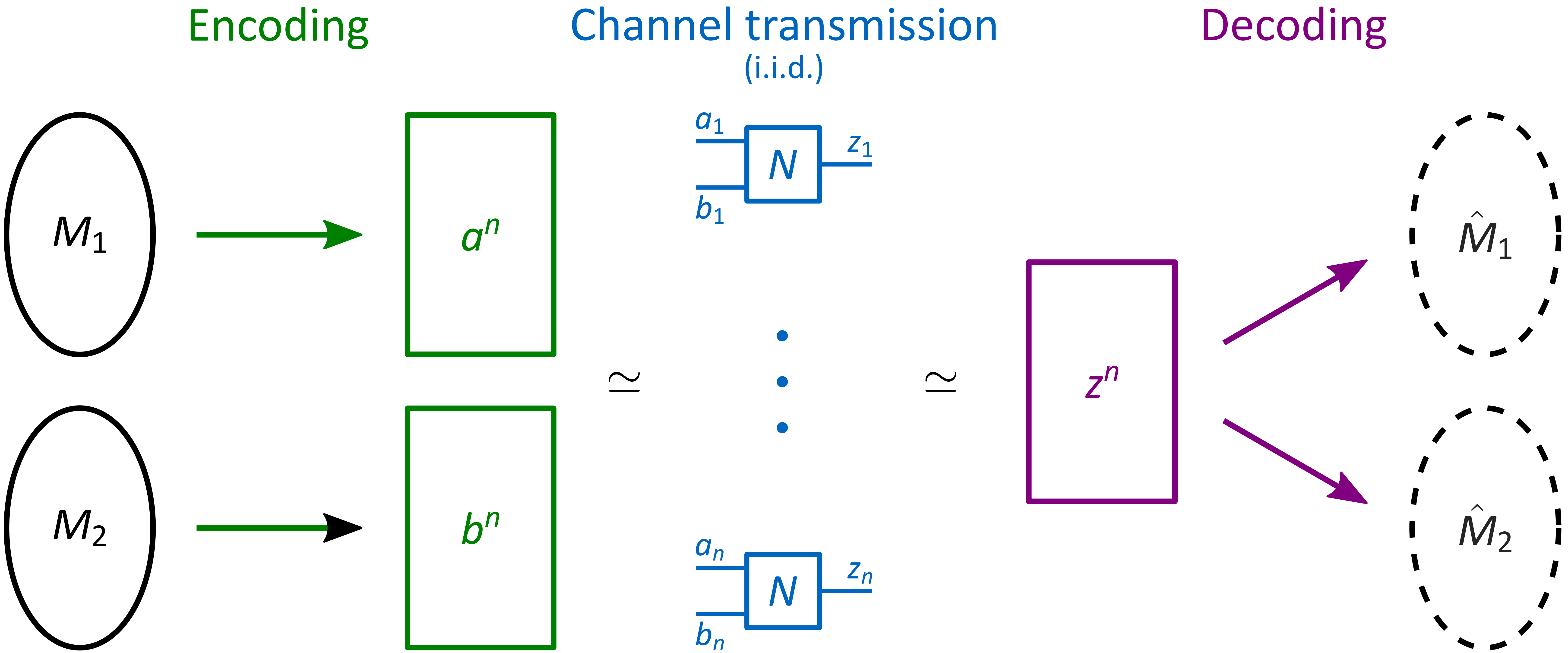
How hard is it to compute the unassisted capacity region of a MAC?

NP-HARD

Talk outline

- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

Coding for a MAC



Codebooks: $|\mathcal{M}_i| = 2^{nR_i}$

Decoding error: $\Pr((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2))$

Capacity region of a MAC

Decoding error: $\varepsilon_n = \Pr((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2))$

Rate tuple (R_1, R_2) for $R_i = \frac{1}{n} \log |\mathcal{M}_i|$ is called *achievable* if $\varepsilon_n \to 0$ as $n \to \infty$.

Capacity region: $\mathcal{C} := \mathrm{cl}\left(\{(R_1, R_2) \text{ achievable}\}\right)$

Single-letter capacity region of a MAC **(Ahlswede '73, Liao '73)**

Let A and B be RVs with product distribution $p_A(a)p_B(b)$, and Z be a RV defined by the MAC N. Then $\mathcal{C}$ is the convex hull of all (R_1, R_2) with

$$R_1 \leq I(A;Z|B) \qquad R_2 \leq I(B;Z|A) \qquad R_1 + R_2 \leq I(AB;Z).$$

Shannon entropy:

$$H(X) = -\sum_x p(x) \log p(x)$$

Mutual information:

$$I(X;Y) = H(X) + H(Y) - H(XY)$$

Conditional mutual information:

$$I(X;Y|Z) = I(X;YZ) - I(X;Z)$$

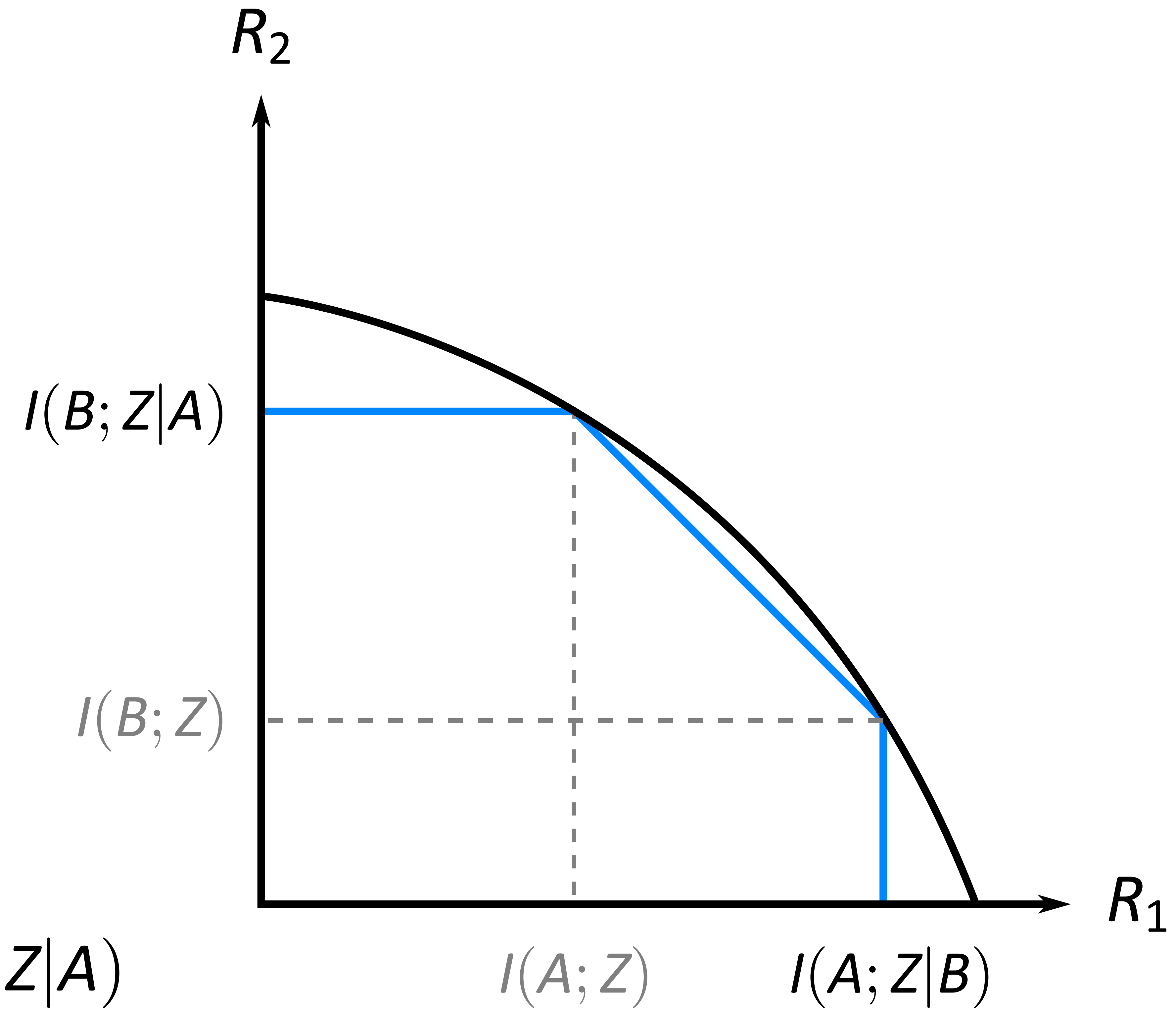
Typical capacity region of a MAC

Constraints for capacity region $\mathcal{C}$:

$$\begin{aligned} R_1 &\leq I(A;Z|B) \\ R_2 &\leq I(B;Z|A) \\ R_1 + R_2 &\leq I(AB;Z). \end{aligned}$$

For fixed product distribution $p_A p_B$ this region is **pentagonal**, since:

$$\begin{aligned} \max\{I(A;Z|B), I(B;Z|A)\} &\leq I(AB;Z) \\ &\leq I(A;Z|B) + I(B;Z|A) \end{aligned}$$



Capacity region of a MAC

Ahlswede-Liao region characterized by **single-letter formula**.

Complicated part: **product constraint** (←independence constraint) on input RVs.

Question 1

Can we use **entanglement assistance** to overcome independence constraint?

Question 2

How hard is it to compute the full region? Product constraint can be turned into **rank-1 constraint.**

[Calvo et al., IEEE Trans. Comm. 58.12 (2010)]

We will study both questions using the theory of **non-local games**.

For simplicity: focus on the **sum rate** $\max\{R_1 + R_2 : (R_1, R_2) \in \mathcal{C}(N)\}$.

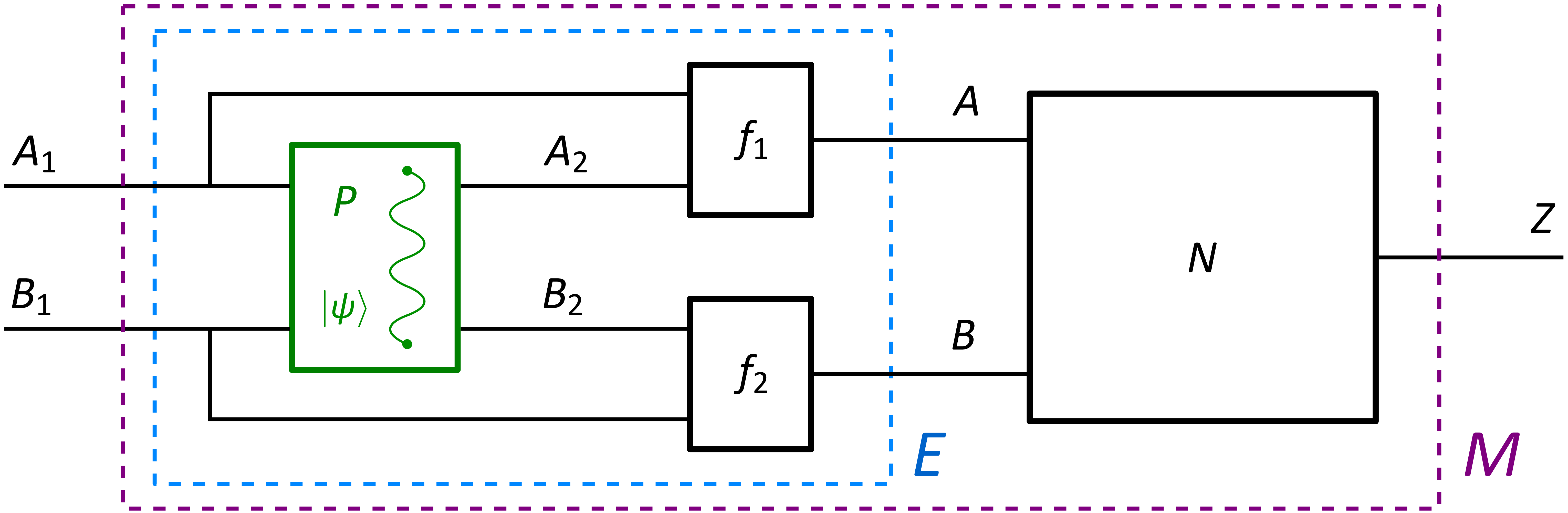
Entanglement assistance for MACs

Senders share entangled state $|\psi\rangle$ and POVMs $\{\Pi_{a_2}^{a_1}\}_{a_2}$ and $\{\Pi_{b_2}^{b_1}\}_{b_2}$:

$$P(a_2, b_2|a_1, b_1) = \langle\psi|\Pi_{a_2}^{a_1} \otimes \Pi_{b_2}^{b_1}|\psi\rangle.$$

Resulting correlation: $E(a, b|a_1, b_1) = f_1(a|a_1, a_2)f_2(b|b_1, b_2)P(a_2, b_2|a_1, b_1)$.

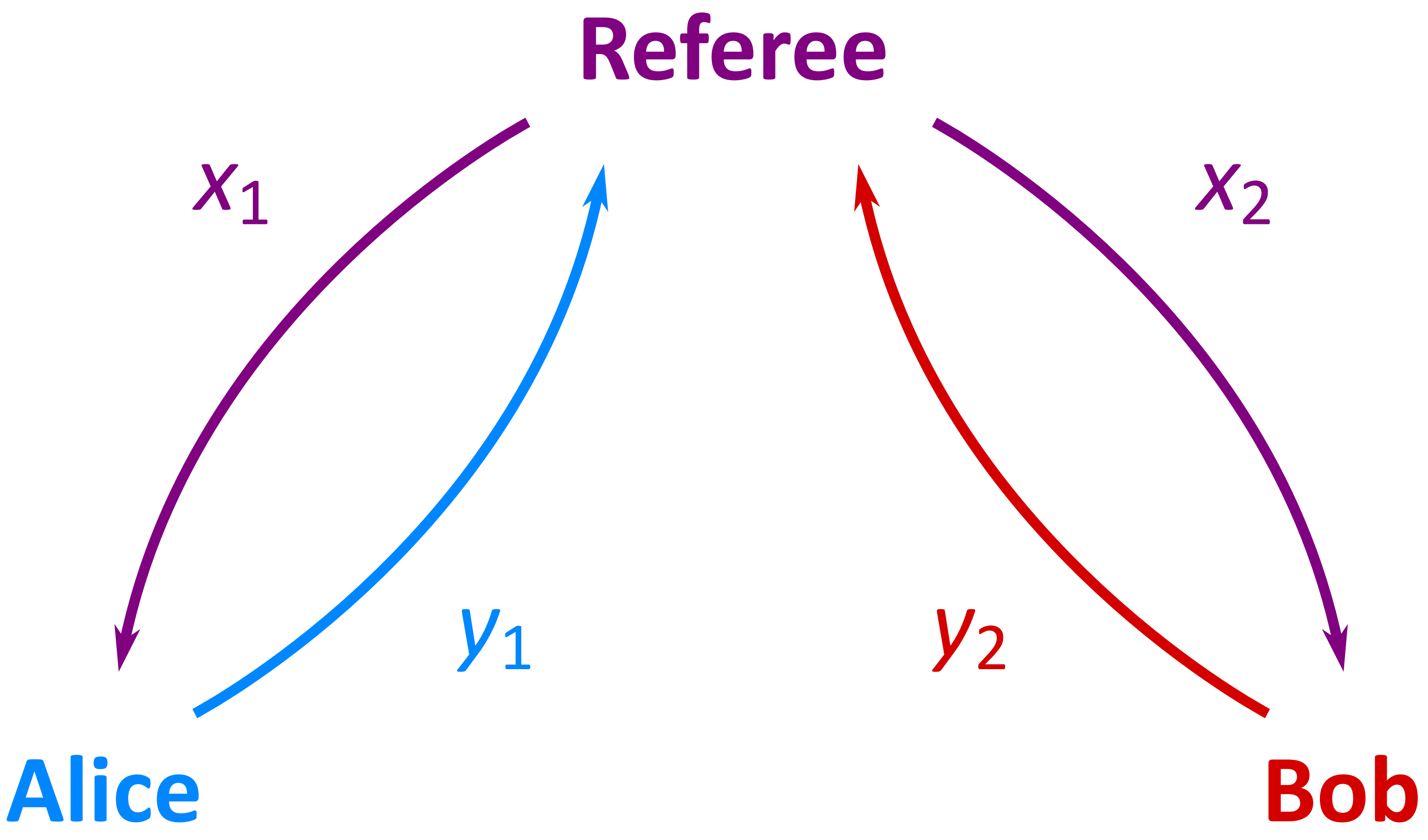
Total MAC: $M = N \circ E$



Talk outline

- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

Non-local games



Questions $x_i \in \mathcal{X}_i$

Answers $y_i \in \mathcal{Y}_i$

Winning condition $W \subseteq \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}_1 \times \mathcal{Y}_2$

Non-local game $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$.

Referee draws questions x_i according to some distribution.

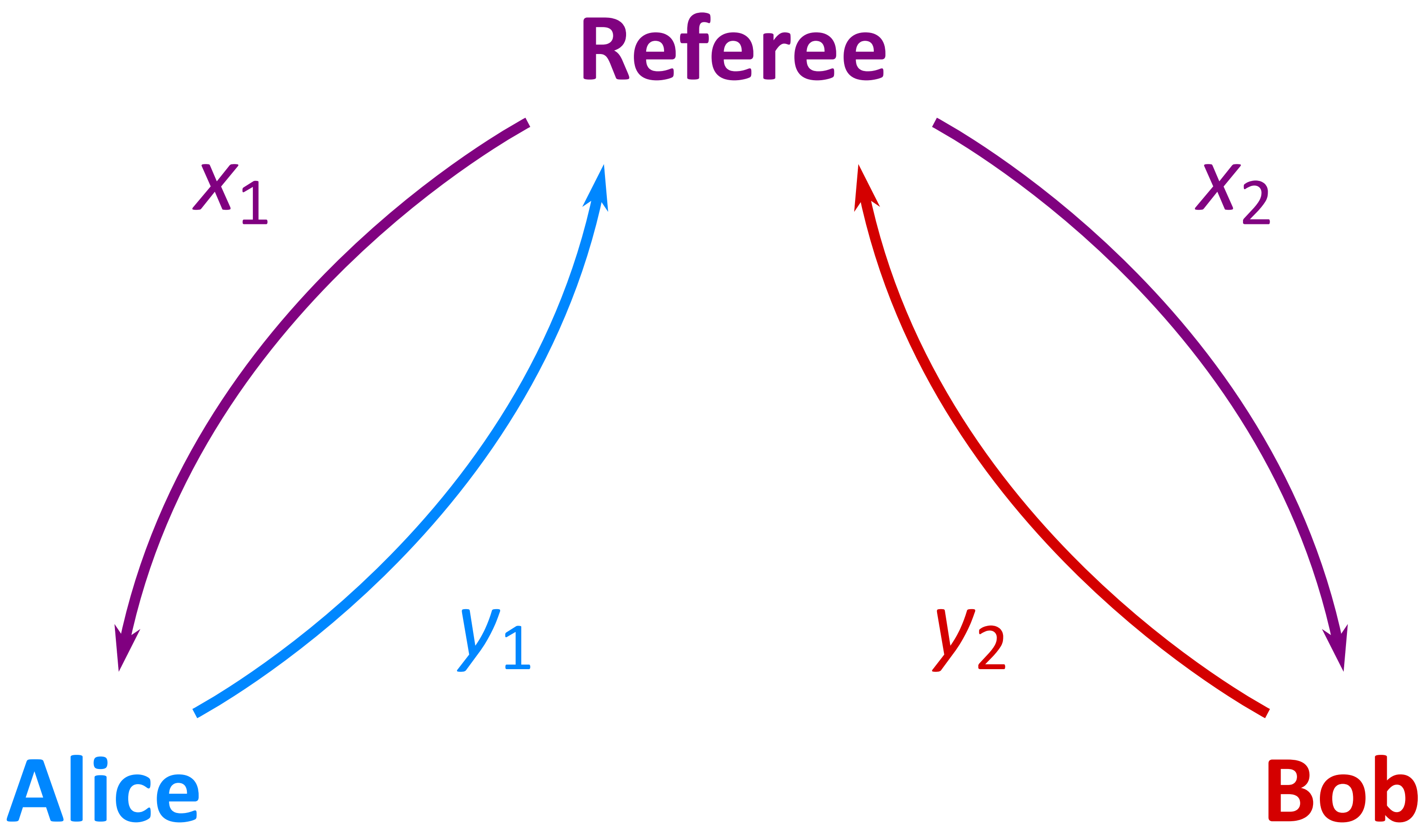
No communication allowed for Alice and Bob to produce answers y_i.

Alice and Bob win if $(x_1, y_1, x_2, y_2) \in W$.

Example: CHSH game

Winning condition: $y_1 \oplus y_2 = x_1 \wedge x_2$

Non-local games: Classical strategies



Questions $x_i \in \mathcal{X}_i$

Answers $y_i \in \mathcal{Y}_i$

Winning condition $W \subseteq \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}_1 \times \mathcal{Y}_2$

Non-local game $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$.

Deterministic strategy:

Deterministic functions $f_i \colon \mathcal{X}_i \to \mathcal{Y}_i$.

Probabilistic strategy:

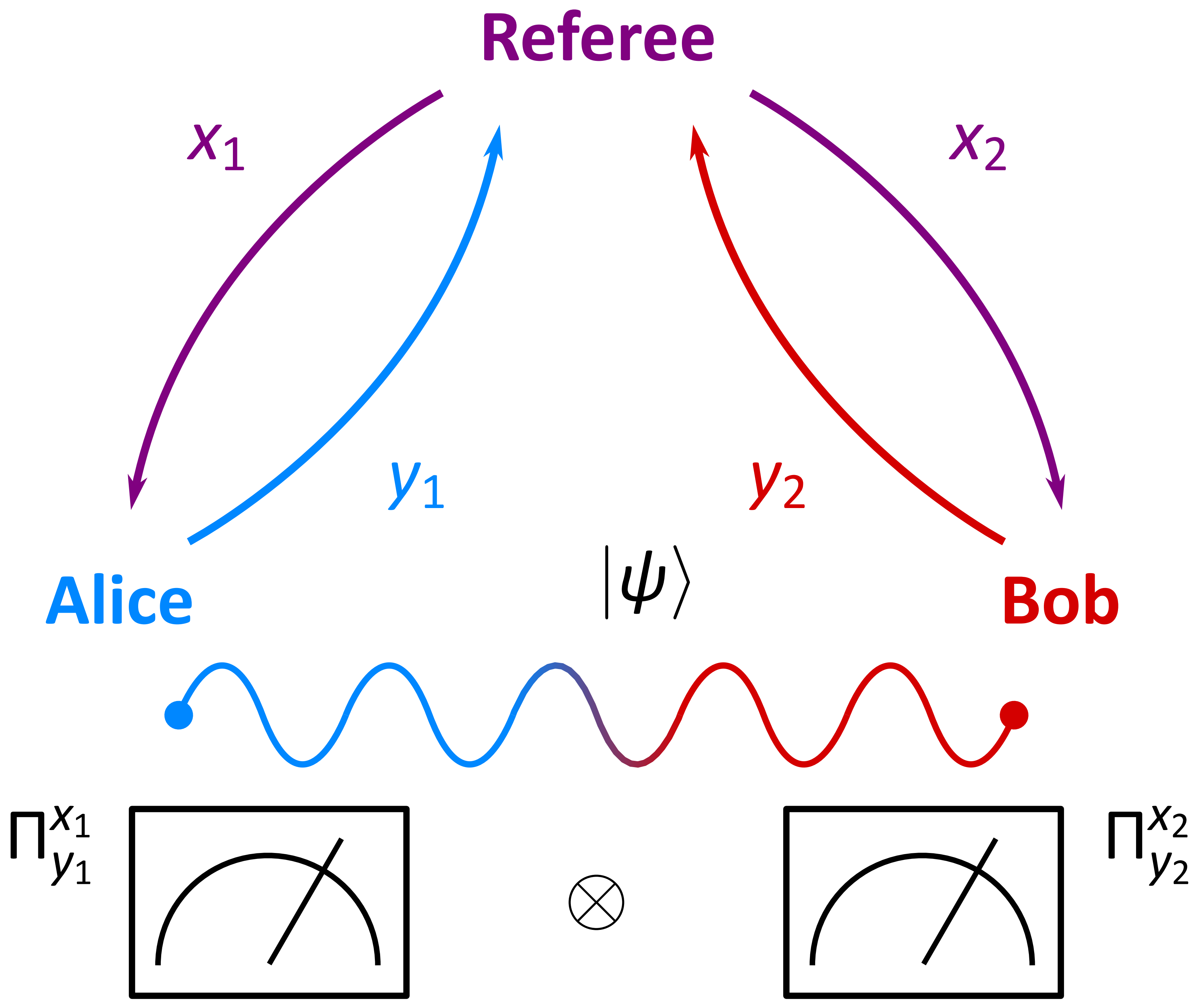
Probabilistic mixture of deterministic strategies.

Classical value $\omega(G)$:

Maximal classical winning probability.

$\omega(G)$ depends on distribution on questions (x_1, x_2).

Non-local games: Quantum strategies



$\Pi^{x_i}_{y_i} \geq 0, \quad \sum_{y_i} \Pi^{x_i}_{y_i} = I$

Quantum strategies:

Alice and Bob share **entangled state** $|\psi\rangle$.

Select **POVMs** $\{\Pi^{x_i}_{y_i}\}_{y_i \in \mathcal{Y}_i}$ for each $x_i \in \mathcal{X}_i$

$(x_1, x_2) \mapsto (y_1, y_2)$ w.p. $\langle\psi|\Pi^{x_1}_{y_1} \otimes \Pi^{x_2}_{y_2}|\psi\rangle$.

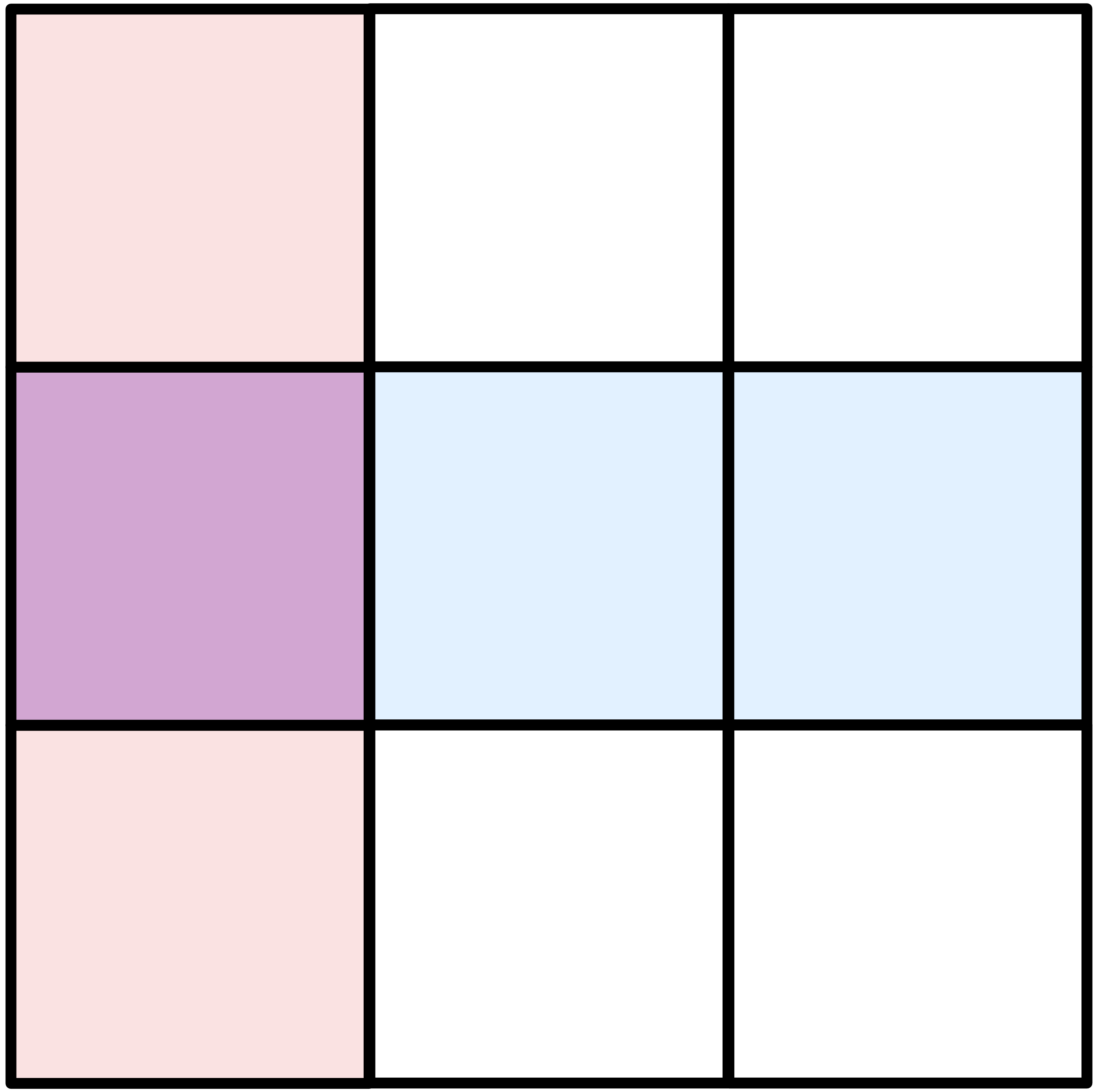
Quantum value $\omega^*(G)$:

maximal quantum winning probability.

Example: CHSH-game G_C

$0.75 = \omega(G_C) < \omega^*(G_C) \approx 0.85$

Magic square game



Alice is given a row.

Bob is given a column.

Both answer with strings of length 3.

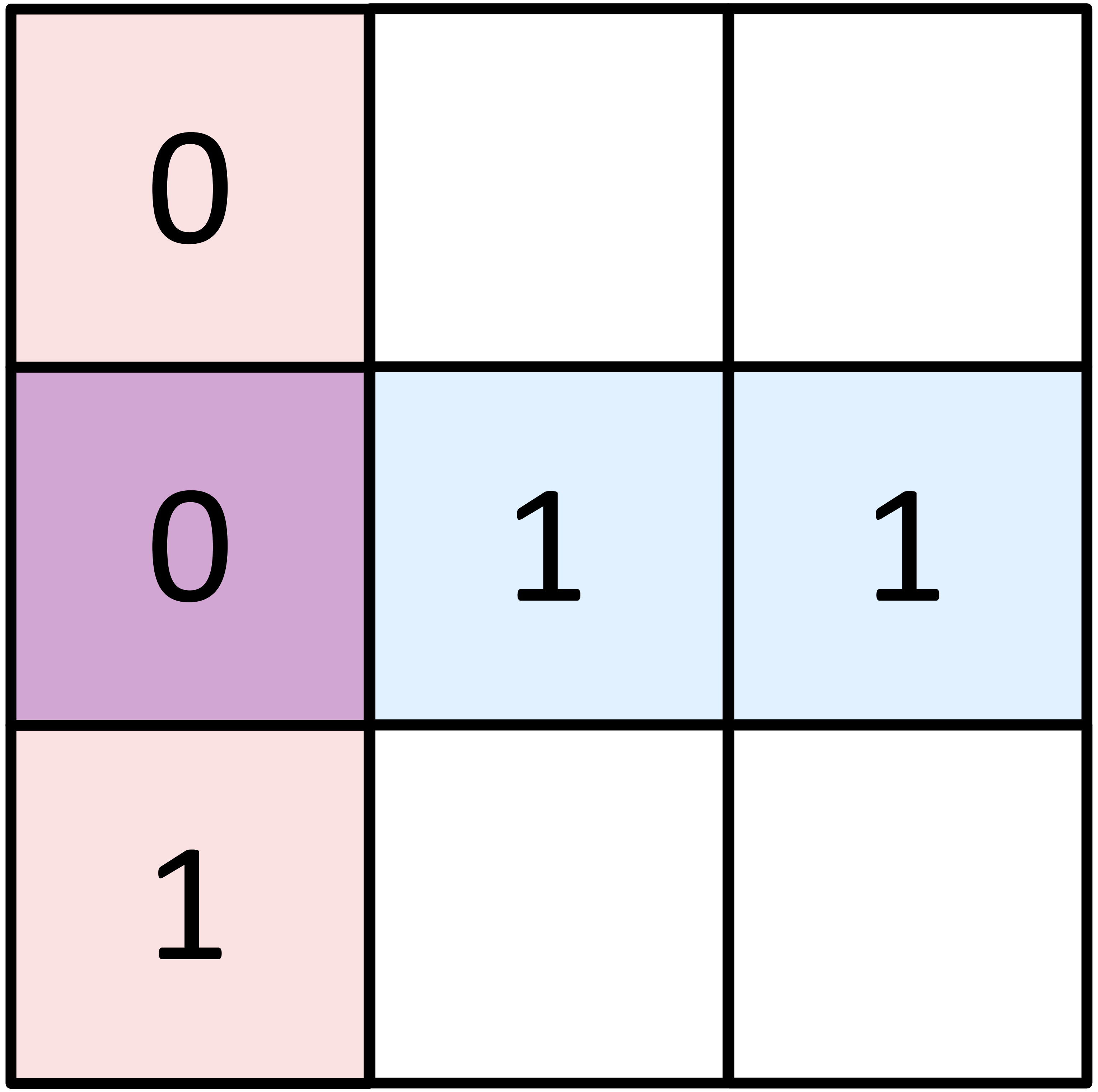
They win, if:

- Alice's parity is even;
- Bob's parity is odd;
- strings agree in overlapping cell.

[Mermin, PRL 65.27 (1990)]

[Peres, Phys. Lett. A 151.3 (1990)]

Magic square game



Alice is given a row.

Bob is given a column.

Both answer with strings of length 3.

They win, if:

- Alice's parity is even;
- Bob's parity is odd;
- strings agree in overlapping cell.

[Mermin, PRL 65.27 (1990)]

[Peres, Phys. Lett. A 151.3 (1990)]

Magic square game

0	0	0
0	1	1
1	0	?

Alice is given a row.

Bob is given a column.

Both answer with strings of length 3.

They win, if:

- Alice's parity is even;
- Bob's parity is odd;
- strings agree in overlapping cell.

[Mermin, PRL 65.27 (1990)]

[Peres, Phys. Lett. A 151.3 (1990)]

MSG: Classical strategies

0	0	0
0	1	1
1	0	?

Perfect deterministic strategy **necessarily violates** parity constraints.

Maximal winning probability: 8/9

For uniformly drawn questions, this also holds for any probabilistic strategy.

Classical value

$\omega(G_{MS}) = 8/9$

[Brassard et al., Found. Phys. 35.11 (2005)]

MSG: A perfect quantum strategy

+XI	+XX	+IX
-XZ	+YY	-ZX
+IZ	+ZZ	+ZI

Let Alice and Bob share two EPR pairs $|\Phi\rangle_{A_1B_1}|\Phi\rangle_{A_2B_2}$, and measure the observables in their row/column.

Observables **commute along rows and columns**.

Parity constraints are **always satisfied**.

Quantum value

$\omega^*(G_{MS}) = 1$

[Mermin, PRL 65.27 (1990)], [Peres, Phys. Lett. A 151.3 (1990)]

[Brassard et al., Found. Phys. 35.11 (2005)]

Talk outline

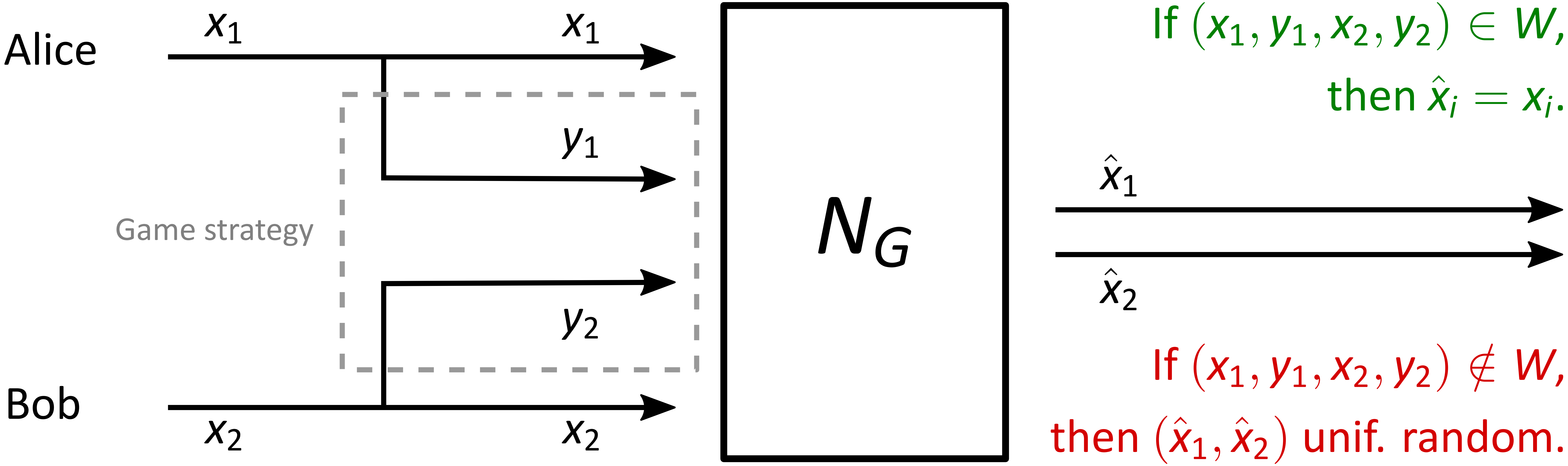
- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

MAC in terms of a non-local game

Let $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$ be a non-local game.

Inputs: question-answer pair (x_i, y_i)

Output: question pair $(\hat{x}_1, \hat{x}_2)$



If $(x_1, y_1, x_2, y_2) \in W$, then $\hat{x}_i = x_i$.

If $(x_1, y_1, x_2, y_2) \notin W$, then $(\hat{x}_1, \hat{x}_2)$ unif. random.

Inspired by [Quek & Shor, PRA 95.5 (2017)].

MAC in terms of a non-local game

Let $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$ be a non-local game.

$$N_G(\hat{x}_1, \hat{x}_2 | x_1, y_1, x_2, y_2) = \begin{cases} \delta(\hat{x}_1, x_1)\delta(\hat{x}_2, x_2) & \text{if } (x_1, y_1, x_2, y_2) \in W \\ (|\mathcal{X}_1||\mathcal{X}_2|)^{-1} & \text{else.} \end{cases}$$

Operational connection to the actual non-local game G:

Alice and Bob ask themselves x_i independently, then produce y_i using a game strategy.

$$\pi(x_1, y_1, x_2, y_2) = \pi(x_1)\pi(x_2)\pi(y_1, y_2 | x_1, x_2)$$

Probabilistic strategies:

$$\pi(y_1, y_2 | x_1, x_2) = \sum_\lambda \pi_\lambda f_1(y_1 | x_1, \lambda) f_2(y_2 | x_2, \lambda)$$

Quantum strategies:

$$\pi(y_1, y_2 | x_1, x_2) = \langle \psi | \Pi_{y_1}^{x_1} \otimes \Pi_{y_2}^{x_2} | \psi \rangle$$

Talk outline

- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

Sum rate of a non-local game MAC

Let $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$ be a non-local game and N_G the MAC derived from it.

Lemma

Let $p_L = \Pr\{(x_1, y_1, x_2, y_2) \notin W)\}$ be the **losing probability**, and set $Z = (\hat{X}_1, \hat{X}_2)$.

Then $R_1 + R_2 \leq I(X_1 Y_1 X_2 Y_2; Z) = H(Z) - p_L(\log|\mathcal{X}_1| + \log|\mathcal{X}_2|)$.

RHS is maximal when:

1) $H(Z) = \log|\mathcal{X}_1| + \log|\mathcal{X}_2|$;
   only possible with sampling x_i uniformly at random!
2) $p_L = 0$.

Problem

For a non-local game G with classical value $\omega(G) < 1$ players **cannot** win on all questions!

Sum rate of a non-local game MAC

Let $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$ be a non-local game and N_G the MAC derived from it.

Lemma

Let $p_L = \Pr\{(x_1, y_1, x_2, y_2) \notin W)\}$ be the **losing probability**, and set $Z = (\hat{X}_1, \hat{X}_2)$.

Then $R_1 + R_2 \leq I(X_1 Y_1 X_2 Y_2; Z) = H(Z) - p_L(\log|\mathcal{X}_1| + \log|\mathcal{X}_2|)$.

Main result: No-Go theorem for classical strategies

For a non-local game with classical value $\omega(G) < 1$,

$$R_1 + R_2 < \log|\mathcal{X}_1| + \log|\mathcal{X}_2|.$$

Sum rate of a non-local game MAC

Let $G = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2, W)$ be a non-local game and N_G the MAC derived from it.

Lemma

Let $p_L = \Pr\{(x_1, y_1, x_2, y_2) \notin W)\}$ be the **losing probability**, and set $Z = (\hat{X}_1, \hat{X}_2)$.

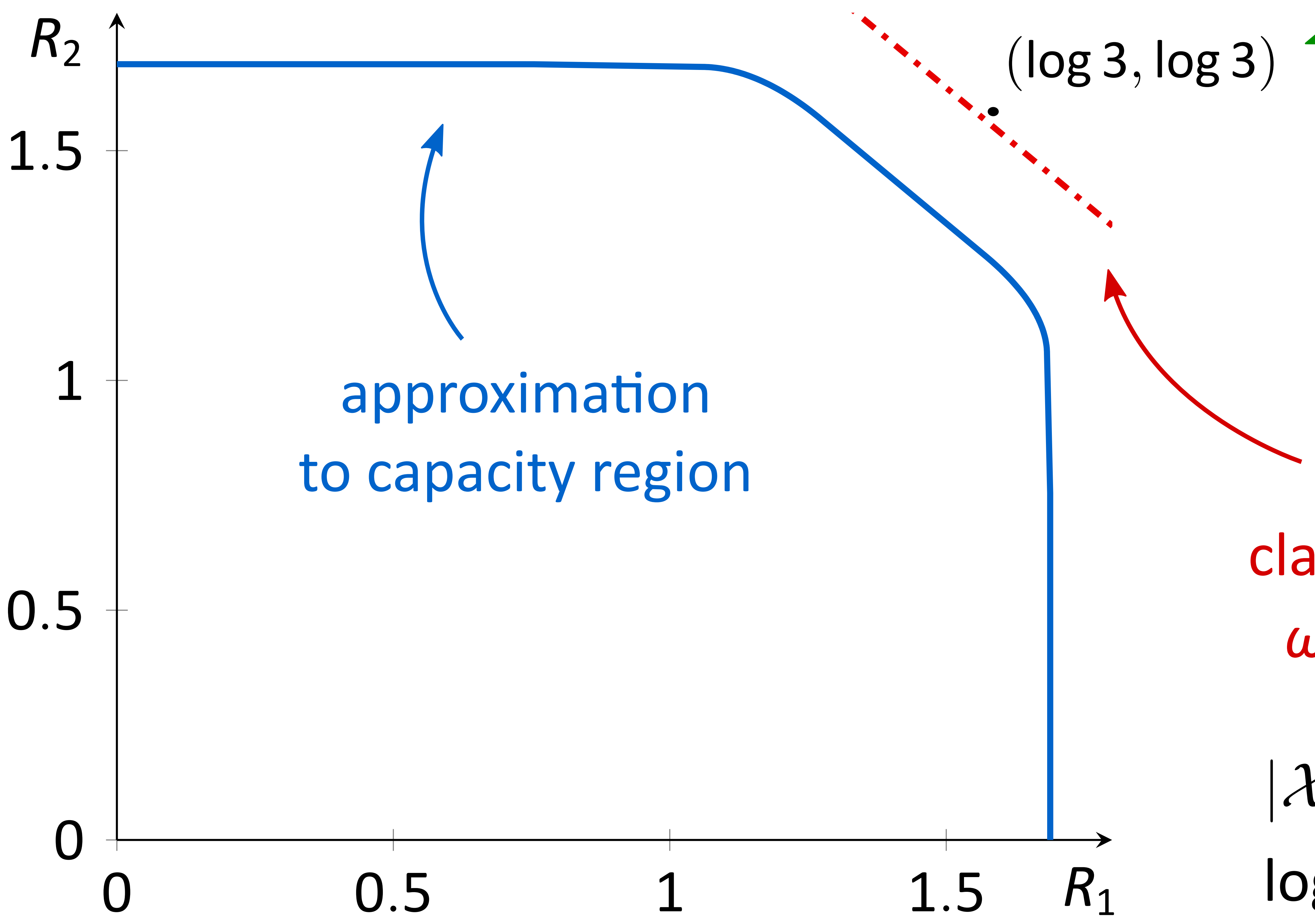
Then $R_1 + R_2 \leq I(X_1 Y_1 X_2 Y_2; Z) = H(Z) - p_L(\log|\mathcal{X}_1| + \log|\mathcal{X}_2|)$.

Main result: perfect sum rate with entanglement

If $\omega^*(G) = 1$, then the **perfect** quantum strategy can be used to **achieve** $(R_1, R_2) = (\log|\mathcal{X}_1|, \log|\mathcal{X}_2|)$ by drawing (x_1, x_2) uniformly at random.

$$\Rightarrow R_1 + R_2 = \log|\mathcal{X}_1| + \log|\mathcal{X}_2|$$

Example: Magic square game channel



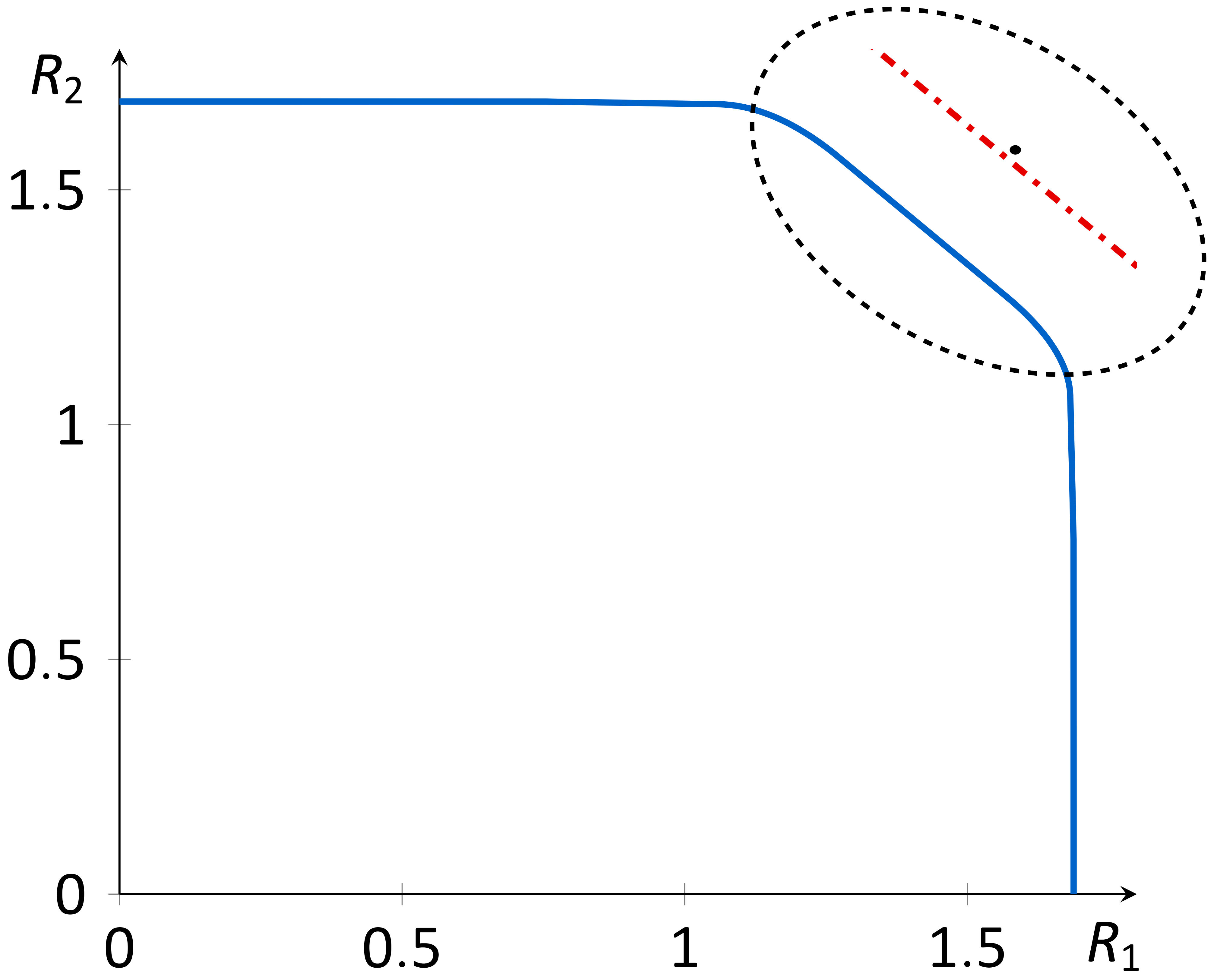
achievable using
perfect quantum strategy
$\omega^*(G_{MS}) = 1$

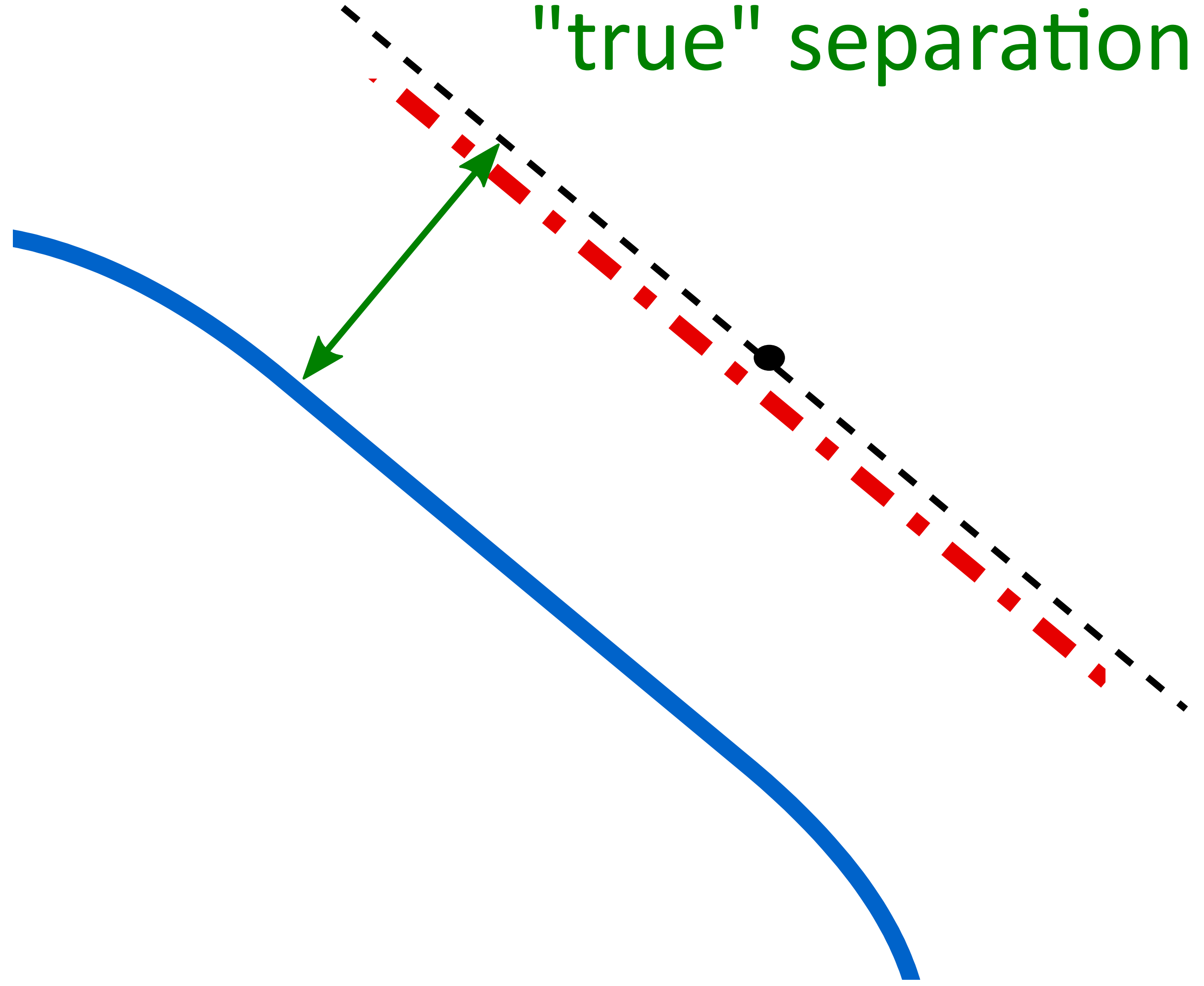
Bound on
classical sum rate
$\omega(G_{MS}) = 8/9$

$|\mathcal{X}_1| = |\mathcal{X}_2| = 3, |\mathcal{Y}_1| = |\mathcal{Y}_2| = 8$

$\log 3 \approx 1.585$

Example: Magic square game channel





Separation from bound: 0.033

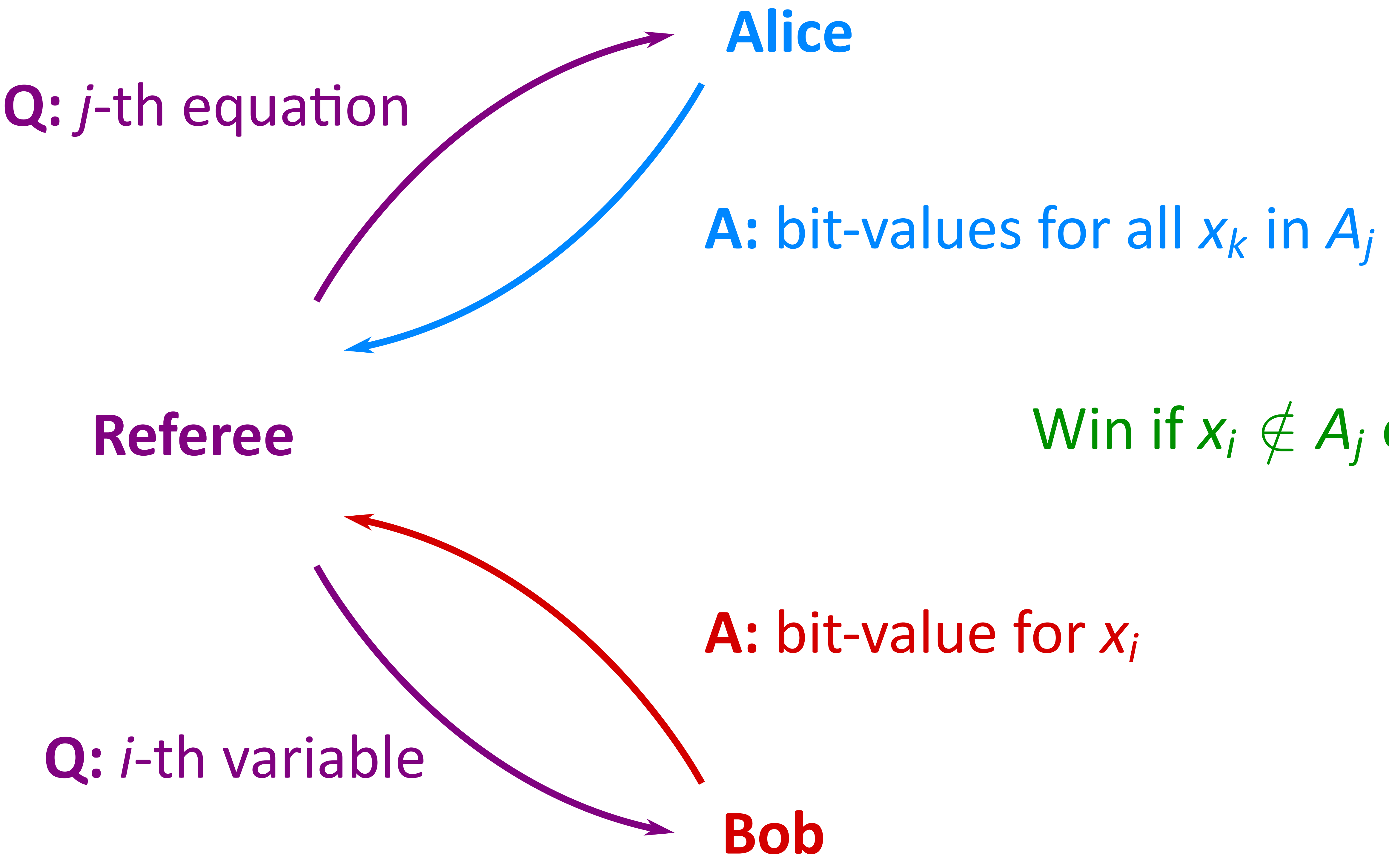
“True” separation: 0.328

Talk outline

- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

Linear system games

Given: Linear system of m equations $Ax = b$ in n variables x_i over $\mathbb{F}_2$.



Win if $x_i \notin A_j$ or answers consistent.

Unbounded entanglement needed

$\exists\, G_{SV} = (A, b)$ such that $\omega^*(G_{SV}) < 1$ for **any finite-dimensional entangled strategy**.

For MES with Schmidt rank d: $\frac{C_1}{d^6} \leq p_L \leq \frac{C_2}{d^2} \Rightarrow$ $\omega^*(G_{SV}) < 1$ for $d < \infty$; $\omega^*(G_{SV}) \to 1$ for $d \to \infty$

Main result: Unbounded entanglement

Any d-entangled strategy for the MAC $N_{G_{SV}}$ must have $R_1 + R_2 < \log m + \log n$.

There is an entangled strategy such that $R_1 + R_2 \to \log m + \log n$ as $d \to \infty$.

For the family of *all* linear system games, it is **undecidable** whether $(\log m, \log n)$ can be achieved for the corresponding family of MACs.

[Slofstra and Vidick, Ann. H. Poincare 19.10 (2018)], [Slofstra, Forum Math. Pi 7 (2019)]

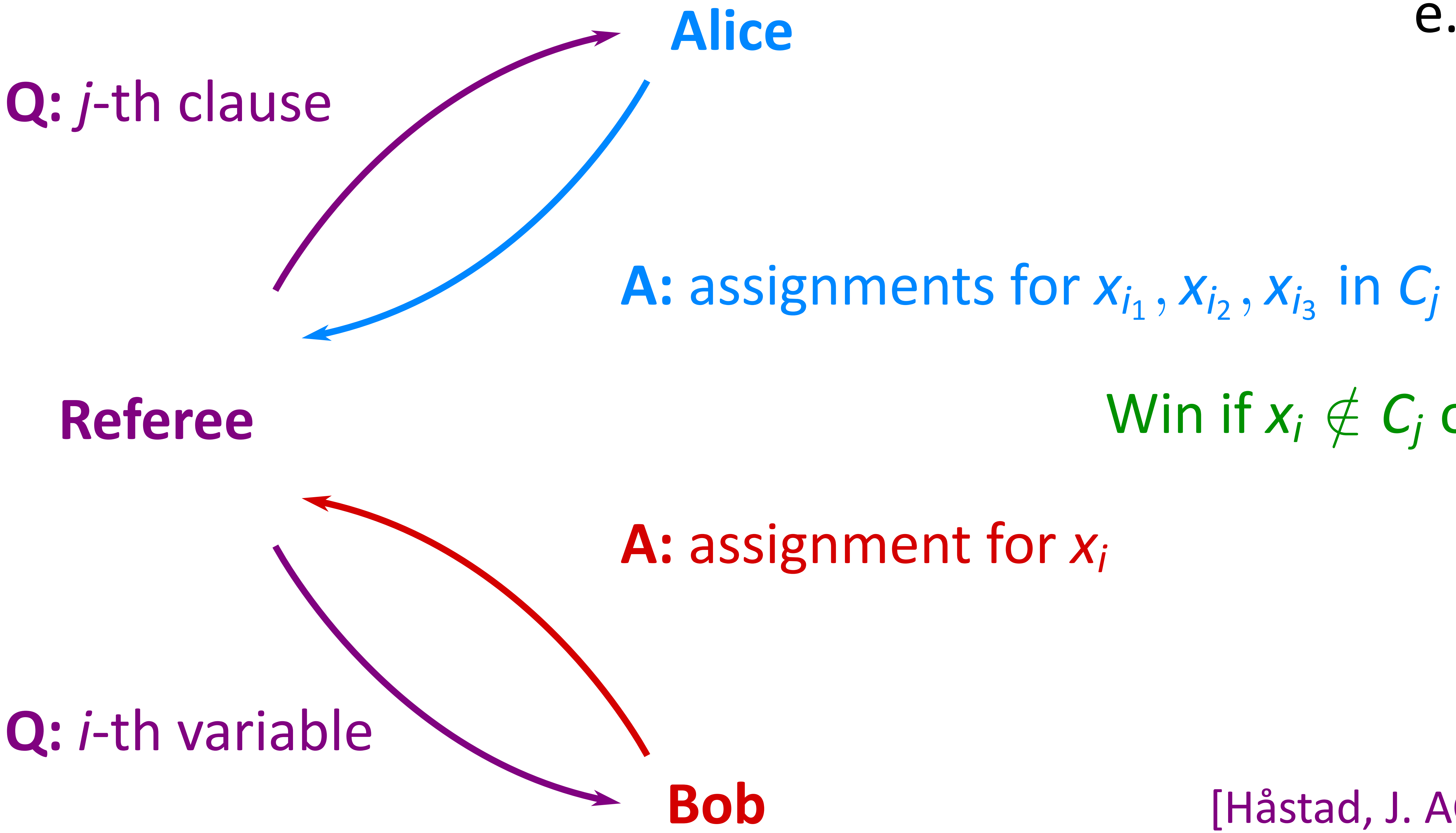
Talk outline

- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

A non-local game version of 3-SAT

Given: Boolean variables $x_1, \ldots, x_n$ and $C_1, \ldots, C_m$ clauses containing exactly 3 literals,

e.g. $C_i = x_2 \vee \neg x_4 \vee x_5$.



Win if $x_i \notin C_j$ or answers consistent.

[Håstad, J. ACM 48.4 (2001)]

NP-hardness of computing capacity region

PCP Theorem: It is NP-hard to decide for Håstad's game G_H with $m = O(n)$ whether $\omega(G_H) = 1$ or $\omega(G_H) \leq 1 - (1-c)/n$ for some $c < 1$.

Main result: NP-hardness of computing unassisted capacity region

For MAC N_{G_H}, it is NP-hard to decide whether $R_1 + R_2 = \log m + \log n$ can be achieved or $R_1 + R_2 \leq \log m + \log n - ((1-c)/n)^3$.

For a point-to-point channel with $O(n)$ bit inputs, we can approximate capacity to precision $O(n^{-3})$ in time $O(n^3 \log n)$ using Blahut-Arimoto algorithm.

With common assumptions about 3-SAT, the scaling for a MAC is $\exp(O(n))$.

Talk outline

- Capacity region of a classical MAC and entanglement assistance
- Quantum correlations and non-local games
- Constructing a MAC in terms of a non-local game
- **Main result 1:** entanglement increases capacity region
- **Main result 2:** unbounded entanglement may be necessary
- **Main result 3:** computing the unassisted capacity region is NP-hard
- Conclusion and open questions

Conclusion

MAC models simple network communication scenario with 2 senders, 1 receiver.

Capacity region given by **single-letter** formula, but **non-convex** problem.

Main results

- Entanglement between senders can boost capacity region of a MAC.
- You may need lots of entanglement to get full boost.
- This is generally undecidable.
- The classical capacity region is NP-hard to compute.

All results are proven by embedding a non-local game in a MAC scenario.

Open questions

Information-theoretic

- Can we improve sum rate bound to get "true" separation?
- Formula for the entanglement-assisted capacity region?
- What about arbitrary (three-way) entanglement assistance?

Optimization-theoretic

- Efficiently computable outer bounds for capacity region of MAC?
- Efficient optimization over (bilinear) quantum strategies?
- Can entanglement boost the capacity of arbitrary MACs?

Thank you

for your attention!