Нові приклади безумовної якісної переваги квантової комунікації над класичною

Д. Гавінський
Інститут математики Академії наук Чеської Республіки
Прага

Комунікаційна складність в теоретичній інформатиці

Комунікаційна складність – одна з найцікавіших моделей обчислення:

Комунікаційна складність в теоретичній інформатиці

Комунікаційна складність – одна з найцікавіших моделей обчислення:

- З одного боку, це одна з найсильніших моделей, де ми вже вміємо доводити (а не лише припускати) *високу складність* (явних) обчислюваних задач – тобто демонструвати *безумовну відсутність ефективних рішень*.

Комунікаційна складність в теоретичній інформатиці

Комунікаційна складність – одна з найцікавіших моделей обчислення:

- З одного боку, це одна з найсильніших моделей, де ми вже вміємо доводити (а не лише припускати) *високу складність* (явних) обчислюваних задач – тобто демонструвати *безумовну відсутність ефективних рішень*.
- З іншого боку, це одна з найслабкіших моделей, де нам відомі достатньо нетривіальні алгоритми – *комунікаційні протоколи*.

Комунікаційна складність в теоретичній інформатиці

Комунікаційна складність – одна з найцікавіших моделей обчислення:

- З одного боку, це одна з найсильніших моделей, де ми вже вміємо доводити (а не лише припускати) *високу складність* (явних) обчислюваних задач – тобто демонструвати *безумовну відсутність ефективних рішень*.
- З іншого боку, це одна з найслабкіших моделей, де нам відомі достатньо нетривіальні алгоритми – *комунікаційні протоколи*.
- Отже, комунікаційна складність є на сьогодні однією з (небагатьох) обчислювальних моделей, де існують *як цікаві ефективні алгоритми в одних випадках, так і докази неможливості їх існування в інших*.

Комунікаційна складність в теоретичній інформатиці

Комунікаційна складність – одна з найцікавіших моделей обчислення:

- З одного боку, це одна з найсильніших моделей, де ми вже вміємо доводити (а не лише припускати) *високу складність* (явних) обчислюваних задач – тобто демонструвати *безумовну відсутність ефективних рішень*.
- З іншого боку, це одна з найслабкіших моделей, де нам відомі достатньо нетривіальні алгоритми – *комунікаційні протоколи*.
- Отже, комунікаційна складність є на сьогодні однією з (небагатьох) обчислювальних моделей, де існують *як цікаві ефективні алгоритми в одних випадках, так і докази неможливості їх існування в інших*.
- Іноді ми знаходимо задачу, що є “занадто важкою” для одного режиму комунікації, але “легкою” для іншого: це є *розділенням* режимів (чи моделей), у такий спосіб ми порівнюємо їх “силу” та показуємо, що один є *якісно сильнішим* за інший (принаймні у деяких випадках).

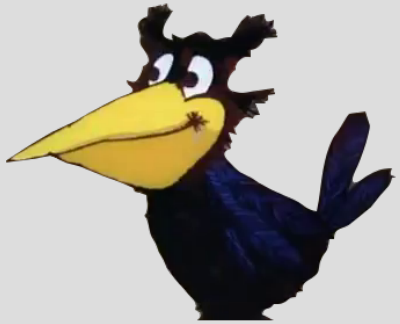
Комунікаційна складність в теоретичній інформатиці

Комунікаційна складність – одна з найцікавіших моделей обчислення:

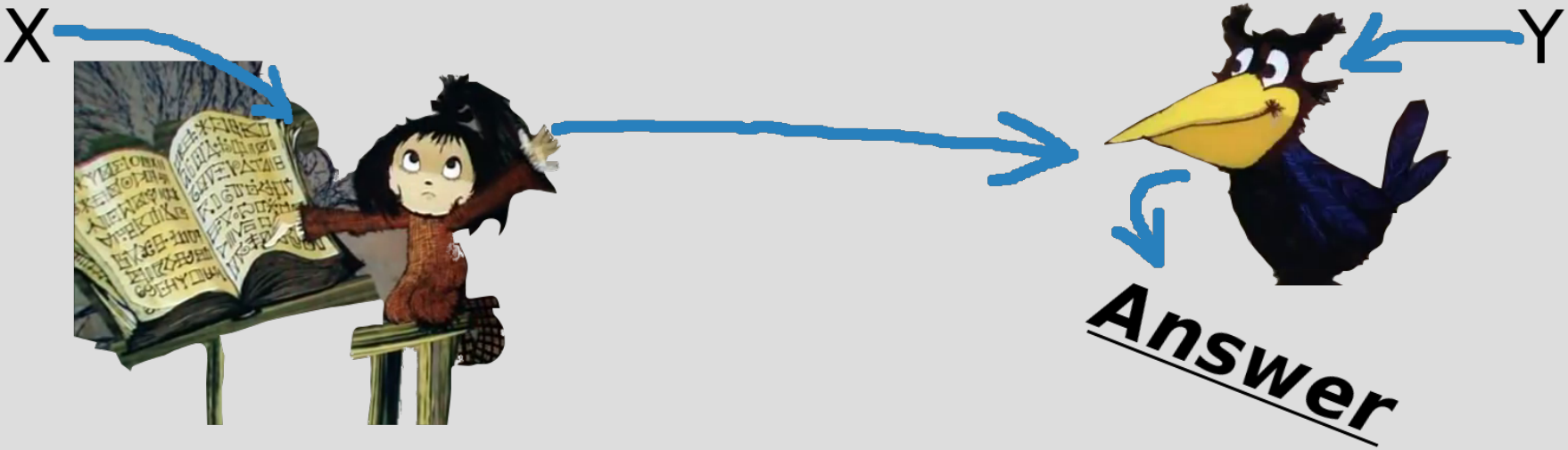
- З одного боку, це одна з найсильніших моделей, де ми вже вміємо доводити (а не лише припускати) *високу складність* (явних) обчислюваних задач – тобто демонструвати *безумовну відсутність ефективних рішень*.
- З іншого боку, це одна з найслабкіших моделей, де нам відомі достатньо нетривіальні алгоритми – *комунікаційні протоколи*.
- Отже, комунікаційна складність є на сьогодні однією з (небагатьох) обчислювальних моделей, де існують *як цікаві ефективні алгоритми в одних випадках, так і докази неможливості їх існування в інших*.
- Іноді ми знаходимо задачу, що є "занадто важкою" для одного режиму комунікації, але "легкою" для іншого: це є *розділенням* режимів (чи моделей), у такий спосіб ми порівнюємо їх "силу" та показуємо, що один є *якісно сильнішим* за інший (принаймні у деяких випадках).
- Зокрема цей підхід може демонструвати ***безумовну якісну перевагу квантової комунікації над класичною***.

  Далі ми розглянемо декілька прикладів таких розділень.

Одностороння комунікація

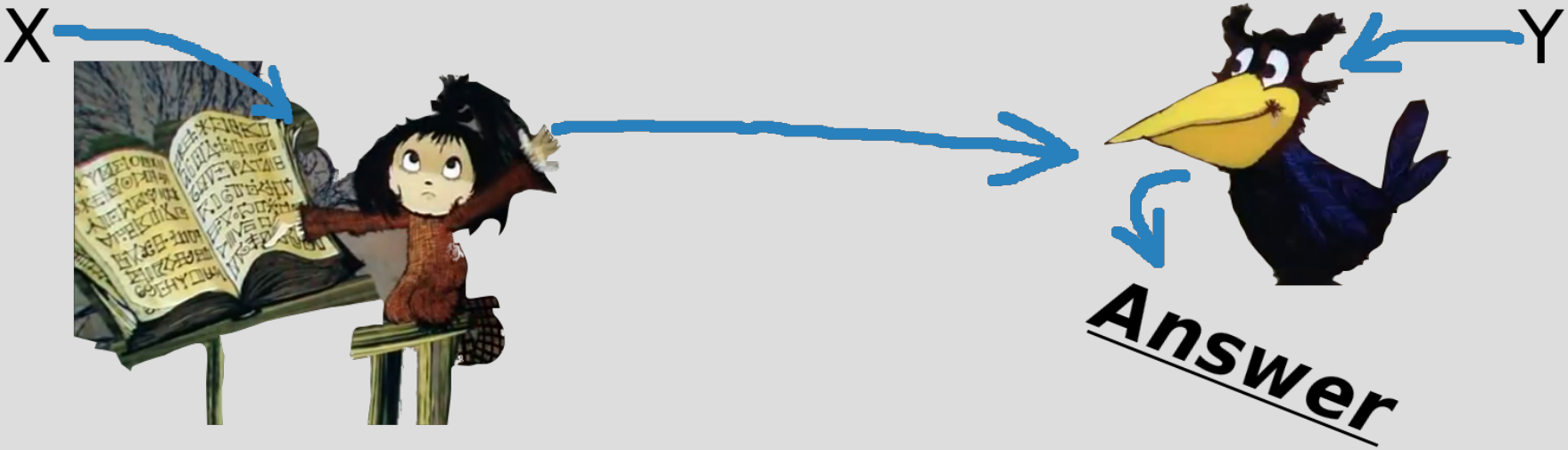


Одностороння комунікація



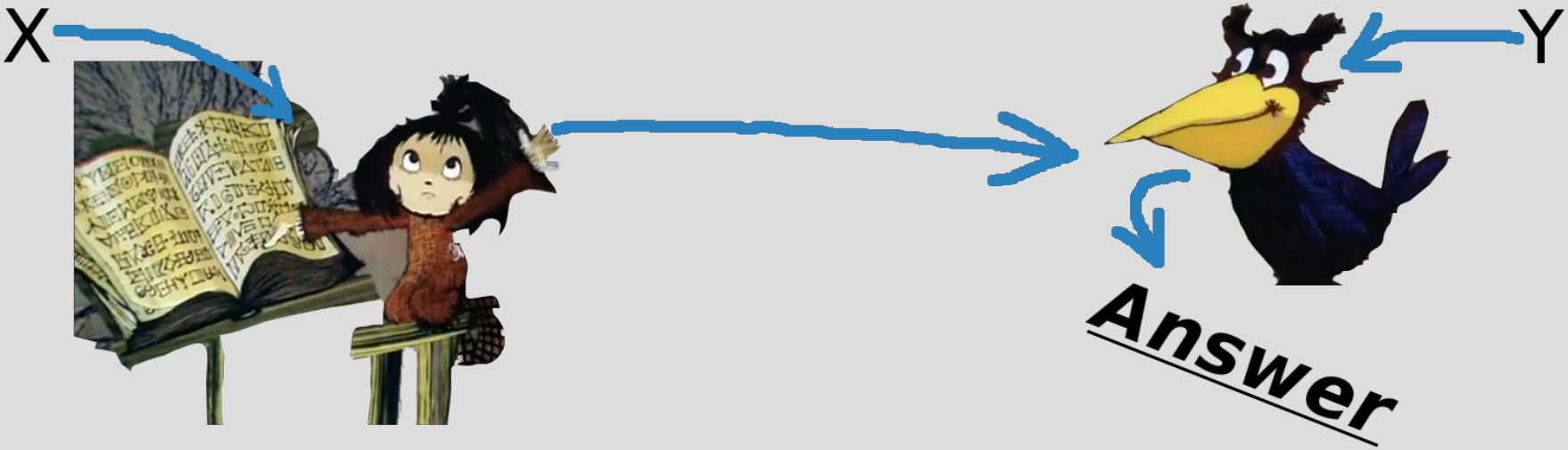
- Аліса отримує вхід X, Боб отримує вхід Y.

Одностороння комунікація



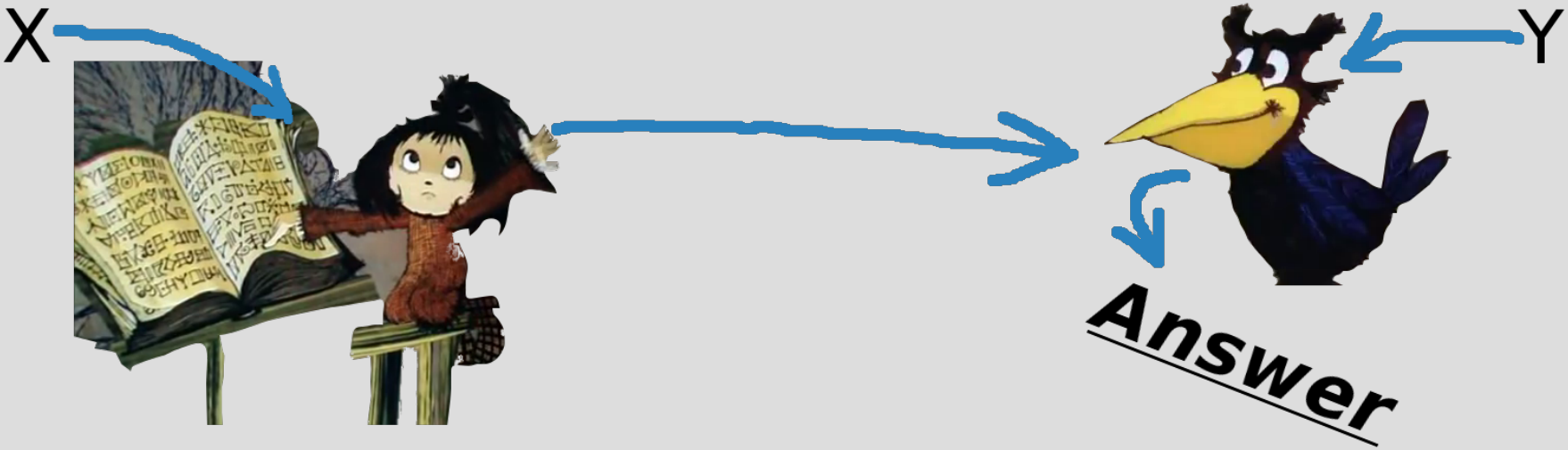
- Аліса отримує вхід X, Боб отримує вхід Y.
- Аліса надсилає Бобові одне повідомлення.

Одностороння комунікація



- Аліса отримує вхід X, Боб отримує вхід Y.
- Аліса надсилає Бобові одне повідомлення.
- Боб видає відповідь, що має погоджуватися з входом (X, Y).

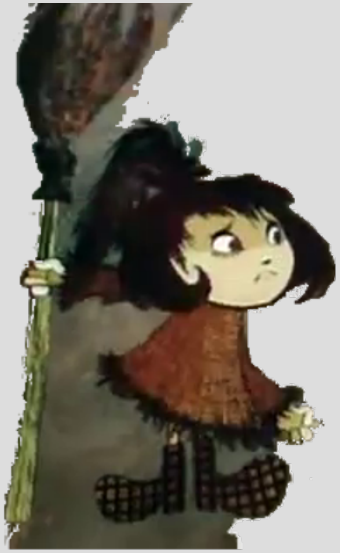
Одностороння комунікація

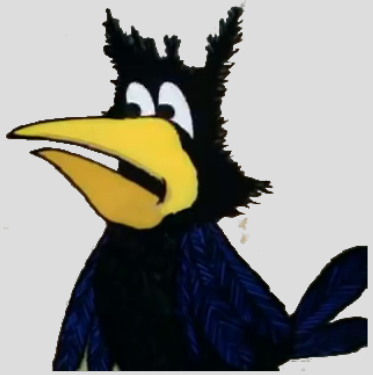


- Аліса отримує вхід X, Боб отримує вхід Y.
- Аліса надсилає Бобові одне повідомлення.
- Боб видає відповідь, що має погоджуватися з входом (X, Y).

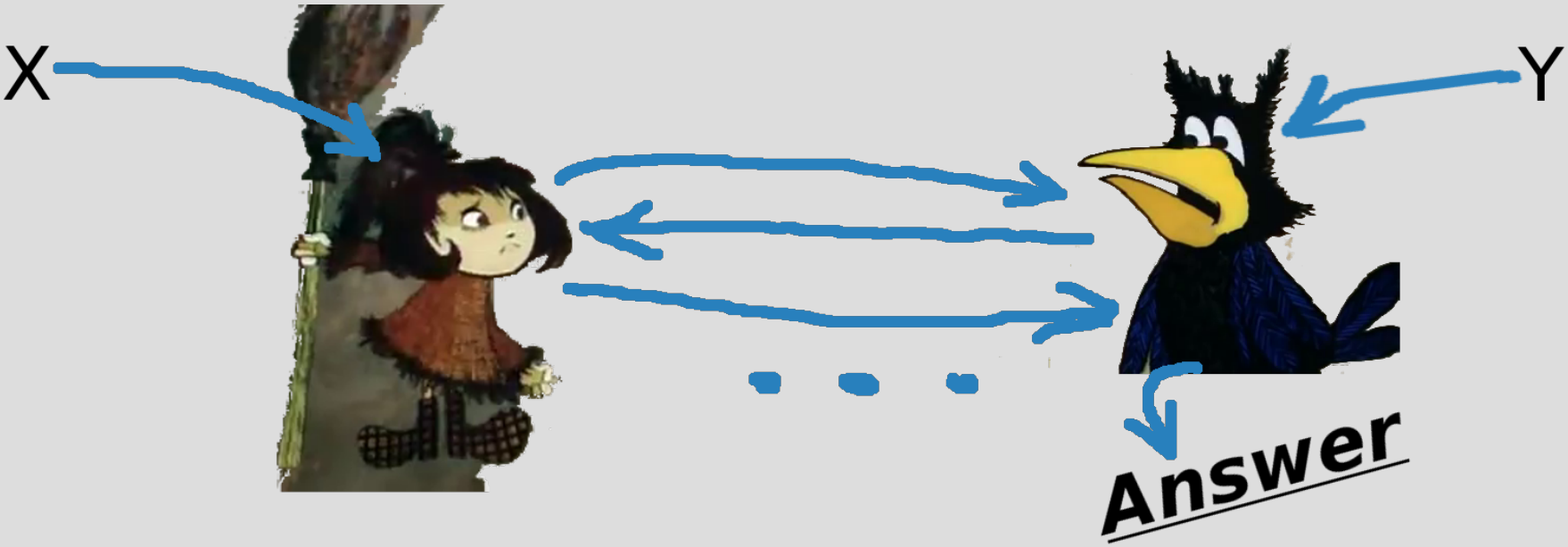
Наприклад, якщо ціллю є обчислення функції двох аргументів $f(\cdot, \cdot)$, то відповіддю має бути значення $f(X, Y)$.

Двостороння комунікація



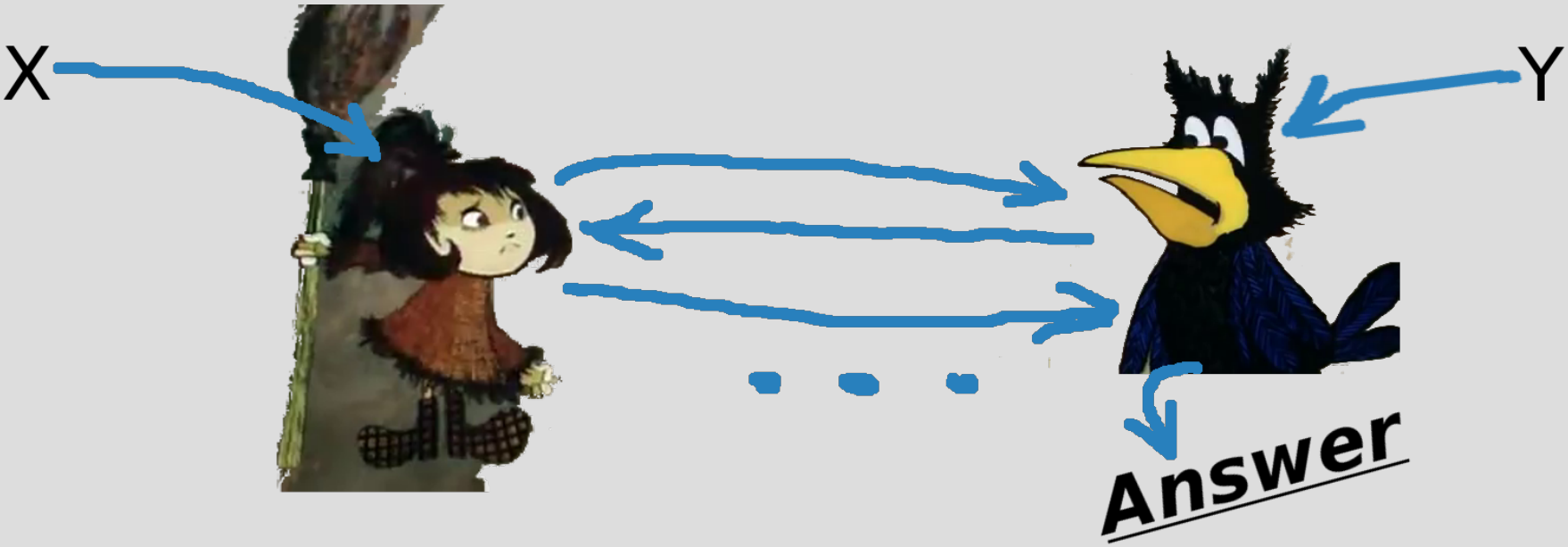


Двостороння комунікація



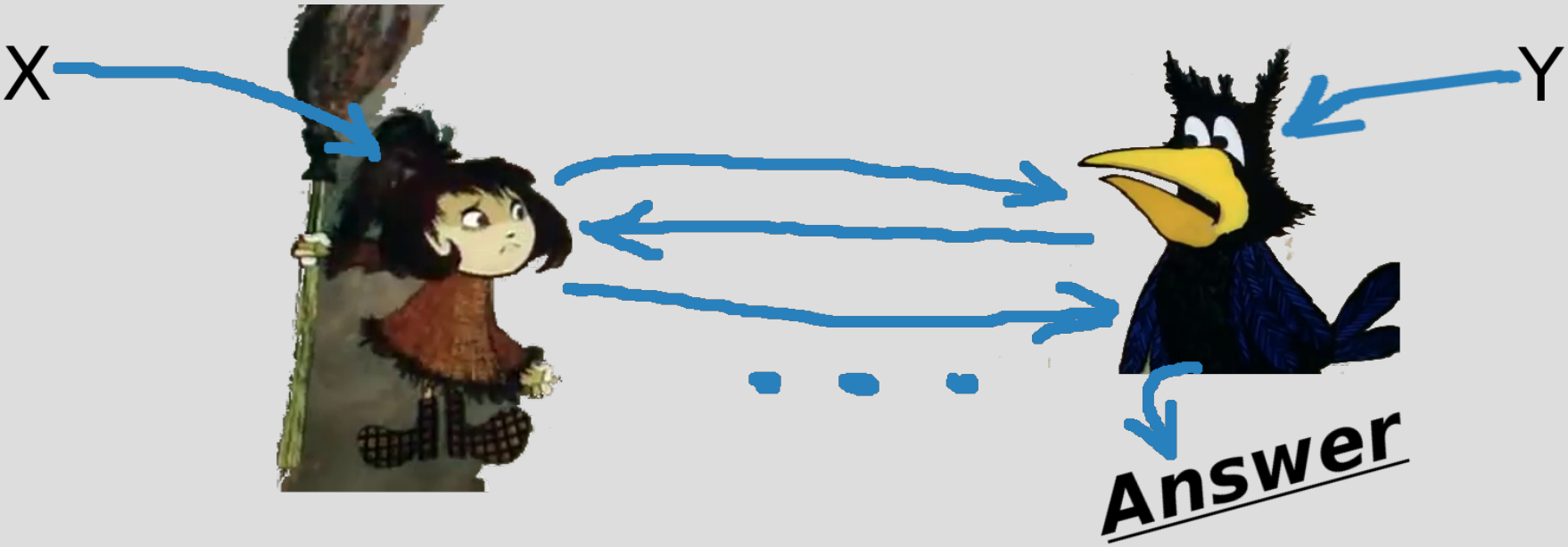
- Аліса отримує вхід X, Боб отримує вхід Y.

Двостороння комунікація



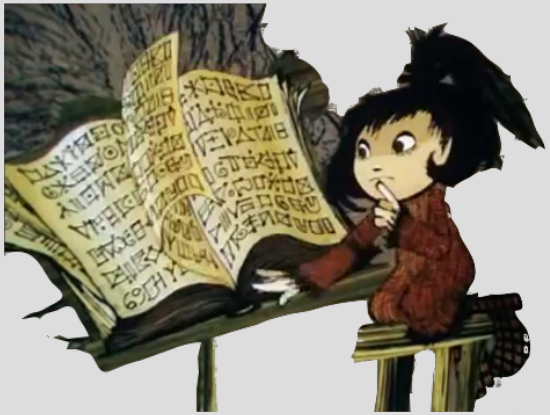
- Аліса отримує вхід X, Боб отримує вхід Y.
- Вони спілкуються.

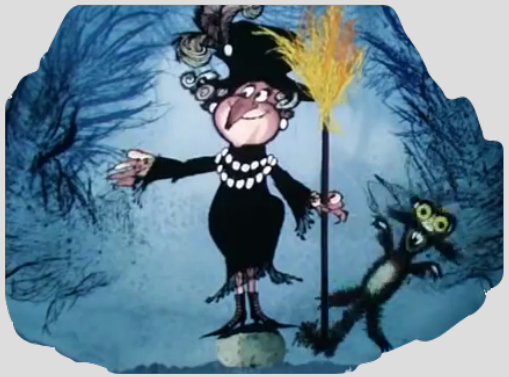
Двостороння комунікація

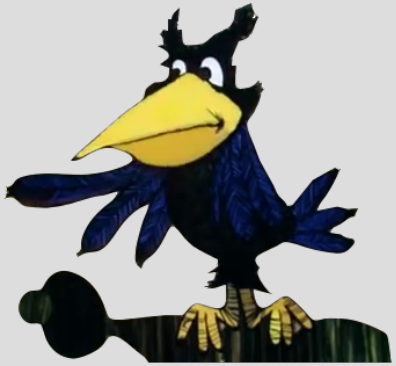


- Аліса отримує вхід X, Боб отримує вхід Y.
- Вони спілкуються.
- Боб видає відповідь, що має погоджуватися з входом (X, Y).

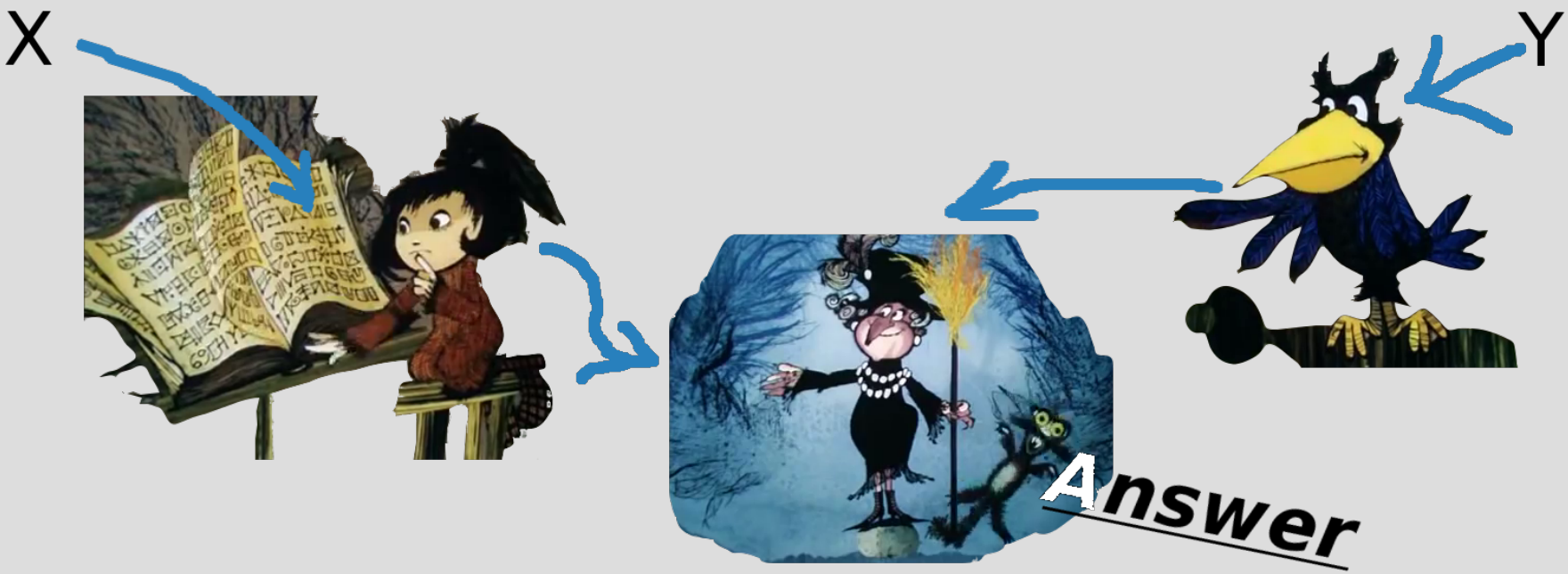
Одночасні повідомлення





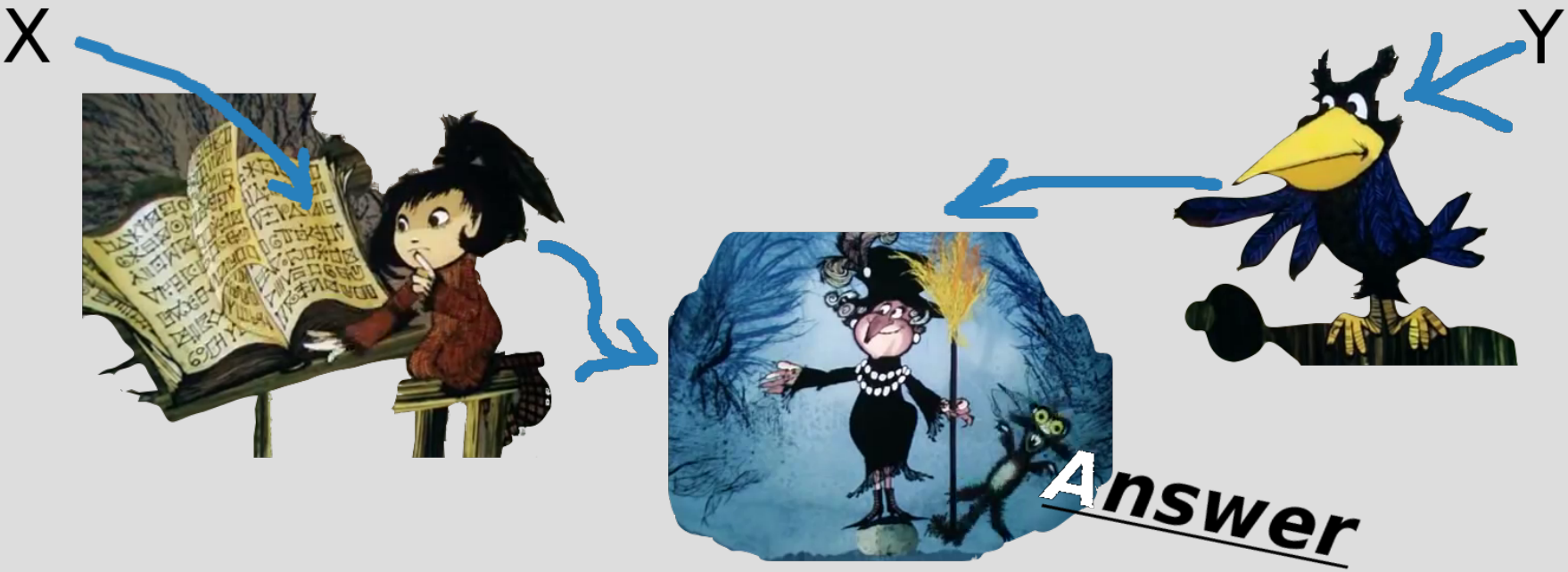


Одночасні повідомлення



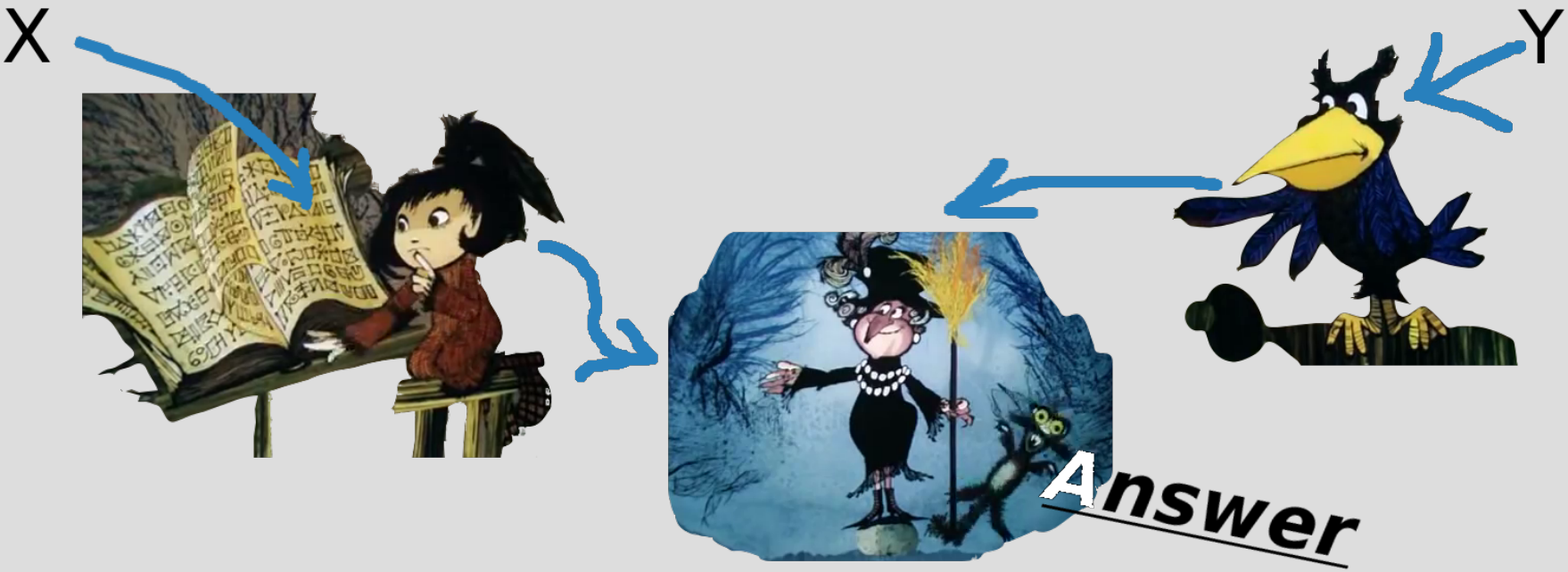
- Аліса отримує вхід X, Боб отримує вхід Y.

Одночасні повідомлення



- Аліса отримує вхід X, Боб отримує вхід Y.
- Аліса та Боб посилають по одному повідомленню до рефері.

Одночасні повідомлення



- Аліса отримує вхід X, Боб отримує вхід Y.
- Аліса та Боб посилають по одному повідомленню до рефері.
- Рефері видає відповідь, що має погоджуватися з входом (X, Y).

Типи та складність комунікаційних протоколів

- Комунікаційні протоколи можуть чи бути *детермінованими*, чи вживати *випадковість* – тобто бути *ймовірнісними*.
  Модель є *посилена поділеною випадковістю* якщо Аліса та Боб можуть “безкоштовно” використовувати *спільні* випадкові біти.

Типи та складність комунікаційних протоколів

- Комунікаційні протоколи можуть чи бути *детермінованими*, чи вживати *випадковість* – тобто бути *ймовірнісними*.
  Модель є *посилена поділеною випадковістю* якщо Аліса та Боб можуть “безкоштовно” використовувати *спільні* випадкові біти.
- Протоколи можуть бути *квантовими*, чи/та бути посилені *поділеною квантовою заплутаністю* (є сильнішою за поділену випадковість).

Типи та складність комунікаційних протоколів

- Комунікаційні протоколи можуть чи бути *детермінованими*, чи вживати *випадковість* – тобто бути *ймовірнісними*.
  Модель є *посилена поділеною випадковістю* якщо Аліса та Боб можуть “безкоштовно” використовувати *спільні* випадкові біти.
- Протоколи можуть бути *квантовими*, чи/та бути посилені *поділеною квантовою заплутаністю* (є сильнішою за поділену випадковість).
- *Складність комунікаційного протоколу* дорівнює загальній кількості бітів чи кубітів, надісланих усіма учасниками.
  Ефективним вважається такий протокол, що його складність *не перевищує полі-логарифмічну* від довжини входу n.

Типи та складність комунікаційних протоколів

- Комунікаційні протоколи можуть чи бути *детермінованими*, чи вживати *випадковість* – тобто бути *ймовірнісними*.
  Модель є *посилена поділеною випадковістю* якщо Аліса та Боб можуть “безкоштовно” використовувати *спільні* випадкові біти.
- Протоколи можуть бути *квантовими*, чи/та бути посилені *поділеною квантовою заплутаністю* (є сильнішою за поділену випадковість).
- *Складність комунікаційного протоколу* дорівнює загальній кількості бітів чи кубітів, надісланих усіма учасниками.
  Ефективним вважається такий протокол, що його складність *не перевищує полі-логарифмічну* від довжини входу n.
- *Складність комунікаційної задачі* (в заданій комунікаційній моделі) дорівнює мінімальної складності такого протоколу, що знаходить правильну відповідь з високою вірогідністю.

Типи та складність комунікаційних протоколів

- Комунікаційні протоколи можуть чи бути *детермінованими*, чи вживати *випадковість* – тобто бути *ймовірнісними*.
  Модель є *посилена поділеною випадковістю* якщо Аліса та Боб можуть “безкоштовно” використовувати *спільні* випадкові біти.
- Протоколи можуть бути *квантовими*, чи/та бути посилені *поділеною квантовою заплутаністю* (є сильнішою за поділену випадковість).
- *Складність комунікаційного протоколу* дорівнює загальній кількості бітів чи кубітів, надісланих усіма учасниками.
  Ефективним вважається такий протокол, що його складність *не перевищує полі-логарифмічну* від довжини входу n.
- *Складність комунікаційної задачі* (в заданій комунікаційній моделі) дорівнює мінімальної складності такого протоколу, що знаходить правильну відповідь з високою вірогідністю.
- Аби довести *якісну перевагу квантових моделей над їх класичними аналогами*, ми розділяємо відповідні комунікаційні режими (тобто моделі): демонструємо таку задачу, що має ефективне рішення у квантовій моделі, але не має в класичній.

Всюди/частково визначені функції; відношення

- Припустимо, Аліса отримує вхід $X \in A$ та Боб отримує вхід $Y \in B$.
  Якщо для кожної пари $(x, y) \in A \times B$ існує *рівно одна правильна відповідь*, тоді ця комунікаційна задача є *всюди визначеною (ВВ) функцією* (відносно області $A \times B$).
  Якщо для кожної пари існує *щонайбільше одна правильна відповідь*, тоді ця задача є *частково визначеною (ЧВ) функцією*.
  Якщо для (всіх чи деяких) пар дозволяються *декілька правильних відповідей*, тоді ця задача є *відношенням*.

Всюди/частково визначені функції; відношення

- Припустимо, Аліса отримує вхід $X \in A$ та Боб отримує вхід $Y \in B$.
  Якщо для кожної пари $(x, y) \in A \times B$ існує *рівно одна правильна відповідь*, тоді ця комунікаційна задача є *всюди визначеною (ВВ) функцією* (відносно області $A \times B$).
  Якщо для кожної пари існує *щонайбільше одна правильна відповідь*, тоді ця задача є *частково визначеною (ЧВ) функцією*.
  Якщо для (всіх чи деяких) пар дозволяються *декілька правильних відповідей*, тоді ця задача є *відношенням*.
- Розділення двох комунікаційних моделей за допомогою ВВ функції є "найпереконливішим" доказом різниці між ними у обчислювальній силі; розділення за допомогою ЧВ функції є дещо слабкішим; розділення за допомогою відношення є найслабшим.

Всюди/частково визначені функції; відношення

- Припустимо, Аліса отримує вхід $X \in A$ та Боб отримує вхід $Y \in B$. Якщо для кожної пари $(x, y) \in A \times B$ існує *рівно одна правильна відповідь*, тоді ця комунікаційна задача є *всюди визначеною (ВВ) функцією* (відносно області $A \times B$).
  Якщо для кожної пари існує *щонайбільше одна правильна відповідь*, тоді ця задача є *частково визначеною (ЧВ) функцією*.
  Якщо для (всіх чи деяких) пар дозволяються *декілька правильних відповідей*, тоді ця задача є *відношенням*.
- Розділення двох комунікаційних моделей за допомогою ВВ функції є "найпереконливішим" доказом різниці між ними у обчислювальній силі; розділення за допомогою ЧВ функції є дещо слабкішим; розділення за допомогою відношення є найслабшим.
- Для деяких пар квантової та класичної комунікаційних моделей нам відомі розділення за допомогою відношень, тоді як розділення за допомогою (ЧВ чи ВВ) функції – неможливе.
  В інших випадках відомим є розділення ЧВ функцією, тоді як можливість розділення ВВ функцією залишається незрозумілою.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: У 1998 році Buhrman, Cleve та Wigderson знайшли *ЧВ функцію*, для якої є ефективний квантовий *безпомилковий* (з можливістю відмови відповідати) двосторонній протокол, але немає класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: У 1999 році Raz знайшов *ЧВ функцію*, для якої є ефективний квантовий двосторонній протокол, але немає класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: У 2001 році Buhrman, Cleve, Watrous та de Wolf знайшли *ВВ функцію*, для якої існує ефективний квантовий одночасний протокол без поділеної випадковості, але не існує класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: У 2004 році Bar-Yossef, Jayram та Kerenidis знайшли *відношення*, що має ефективний квантовий односторонній протокол, але не має класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: У 2007 році у співпраці з Kempe, Kerenidis, Raz та de Wolf те ж саме було досягнуто за допомогою *ЧВ функції*.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*GKKRdW07*] – *ЧВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: У 2008 році було знайдено *відношення*, для якого існує ефективний односторонній квантовий протокол, але немає (навіть) двостороннього класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*GKKRdW07*] – *ЧВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*2008*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: У 2010 році Klartag та Regev продемонстрували таке саме розділення за допомогою *ЧВ функції*.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*GKKRdW07*] – *ЧВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*2008*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*KR10*] – *ЧВ функція*
- $\mathcal{Q}^{\|,ent}$ vs. $\mathcal{R}$: У 2016 році було знайдено *ЧВ функцію*, яка має ефективний одночасний квантовий протокол з заплутаністю, але не має (навіть) двостороннього класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*GKKRdW07*] – *ЧВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*2008*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*KR10*] – *ЧВ функція*
- $\mathcal{Q}^{\|,ent}$ vs. $\mathcal{R}$: [*2016*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|,pub}$: У 2018 році було знайдено *ЧВ функцію*, яка має ефективний одночасний квантовий протокол без поділеної випадковості, але не має одночасного класичного (навіть) з поділеною випадковістю.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*GKKRdW07*] – *ЧВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*2008*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*KR10*] – *ЧВ функція*
- $\mathcal{Q}^{\|,ent}$ vs. $\mathcal{R}$: [*2016*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|,pub}$: [*2018*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: У 2020 році було знайдено *відношення*, для якого існує ефективний одночасний квантовий протокол (без поділеної заплутаності чи випадковості), але немає (навіть) двостороннього класичного.

Приклади переваги квантової комунікації над класичною

N.B. Усі двосторонні моделі є сильніші, ніж їх односторонні аналоги, котрі, у свою чергу, сильніші за SMP (одночасні повідомлення).

- $\mathcal{Q}$ vs. $\mathcal{R}$: [*BCW98*] – *ЧВ функція*, *безпомилковий*
- $\mathcal{Q}$ vs. $\mathcal{R}$: [*Raz99*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|}$: [*BCWdW01*] – *ВВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*BJK04*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}^{1}$: [*GKKRdW07*] – *ЧВ функція*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*2008*] – *відношення*
- $\mathcal{Q}^{1}$ vs. $\mathcal{R}$: [*KR10*] – *ЧВ функція*
- $\mathcal{Q}^{\|,ent}$ vs. $\mathcal{R}$: [*2016*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}^{\|,pub}$: [*2018*] – *ЧВ функція*
- $\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: [*2020*] – *відношення*

$\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: The Gap Hamming Relation (*GHR*)

- Let n be *a power of* 2 and $\{\tau_1, \ldots, \tau_n\} \subset \{\pm 1\}^n$ be an orthogonal set of vectors (corresponding to a Fourier basis for $\{0,1\}^{\log n} \to \{\pm 1\}$).

$\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: The Gap Hamming Relation (*GHR*)

- Let n be *a power of* 2 and $\{\tau_1, \ldots, \tau_n\} \subset \{\pm 1\}^n$ be an orthogonal set of vectors (corresponding to a Fourier basis for $\{0,1\}^{\log n} \to \{\pm 1\}$).
- For $j \in [n]$, let σ_j denote *the j'th cyclic shift* of an n-bit string.

$\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: The Gap Hamming Relation (*GHR*)

- Let n be *a power of* 2 and $\{\tau_1, \ldots, \tau_n\} \subset \{\pm 1\}^n$ be an orthogonal set of vectors (corresponding to a Fourier basis for $\{0,1\}^{\log n} \to \{\pm 1\}$).
- For $j \in [n]$, let σ_j denote *the j'th cyclic shift* of an n-bit string.
- For $x \in \{0,1\}^n$ and $j, s \in [n]$, denote: $\rho_{j,s}(x) \stackrel{\text{def}}{=} \sigma_j(\tau_s \oplus x)$, where $\oplus$ is an element-wise operation defined via $1 \oplus a = a$ and $-1 \oplus a = \neg a$.

$\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: The Gap Hamming Relation (*GHR*)

- Let n be *a power of* 2 and $\{\tau_1, \ldots, \tau_n\} \subset \{\pm 1\}^n$ be an orthogonal set of vectors (corresponding to a Fourier basis for $\{0,1\}^{\log n} \to \{\pm 1\}$).
- For $j \in [n]$, let σ_j denote *the j'th cyclic shift* of an n-bit string.
- For $x \in \{0,1\}^n$ and $j, s \in [n]$, denote: $\rho_{j,s}(x) \stackrel{\text{def}}{=} \sigma_j(\tau_s \oplus x)$, where $\oplus$ is an element-wise operation defined via $1 \oplus a = a$ and $-1 \oplus a = \neg a$.
- The input to the *Gap Hamming Relation (GHR)* is a pair (x, y) of n-bit strings, and the output is a sequence $(j_1, s_1), \ldots, (j_{\log n}, s_{\log n})$.
  Such a sequence is *a valid answer to* $GHR(x, y)$ if *at least half of the corresponding transformations* ρ_{j_i,s_i} map the value of x either *somewhat close to* or *somewhat far from* the value of y in terms of the *Hamming distance*.

$\mathcal{Q}^{\|}$ vs. $\mathcal{R}$: The Gap Hamming Relation (*GHR*)

- Let n be *a power of* 2 and $\{\tau_1, \ldots, \tau_n\} \subset \{\pm 1\}^n$ be an orthogonal set of vectors (corresponding to a Fourier basis for $\{0,1\}^{\log n} \to \{\pm 1\}$).
- For $j \in [n]$, let σ_j denote *the j'th cyclic shift* of an n-bit string.
- For $x \in \{0,1\}^n$ and $j, s \in [n]$, denote: $\rho_{j,s}(x) \stackrel{\text{def}}{=} \sigma_j(\tau_s \oplus x)$, where $\oplus$ is an element-wise operation defined via $1 \oplus a = a$ and $-1 \oplus a = \neg a$.
- The input to the *Gap Hamming Relation (GHR)* is a pair (x, y) of n-bit strings, and the output is a sequence $(j_1, s_1), \ldots, (j_{\log n}, s_{\log n})$.
  Such a sequence is *a valid answer to* $GHR(x, y)$ if *at least half of the corresponding transformations* ρ_{j_i,s_i} map the value of x either *somewhat close to* or *somewhat far from* the value of y in terms of the *Hamming distance*.
- Formally, $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if

$$\begin{cases} \left| \left\{ i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2} \right] \right\} \right| \geq \frac{\log n}{2} & \text{if } \aleph(x, y); \\ \top & \text{otherwise,} \end{cases}$$

where $\aleph(\mathcal{X}, \mathcal{Y})$ is certain predicate that is satisfied almost always for uniformly-random $(\mathcal{X}, \mathcal{Y})$.

GHR is easy for quantum *SMP*

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

GHR is easy for quantum *SMP*

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that “favours” correct answers*:

GHR is easy for quantum *SMP*

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that “favours” correct answers*:

- Let $|1\rangle, \ldots, |n\rangle$ be an orthonormal basis for the space $\mathbb{R}^n$ of $\log n$ *qubits*.

GHR is easy for quantum *SMP*

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Let $|1\rangle, \ldots, |n\rangle$ be an orthonormal basis for the space $\mathbb{R}^n$ of $\log n$ *qubits*.
- Let Alice and Bob send to the referee $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.

GHR is easy for quantum *SMP*

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Let $|1\rangle, \ldots, |n\rangle$ be an orthonormal basis for the space $\mathbb{R}^n$ of $\log n$ *qubits*.
- Let Alice and Bob send to the referee $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.
- Denote for $j, s \in [n]$: $u_j^s \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{\frac{\tau_s|_i + 1}{2}} \cdot |i\rangle \otimes |\sigma_j(i)\rangle \ \ (\in \mathbb{R}^{n^2})$, where $\sigma_j(i) \stackrel{\text{def}}{=} i + j \mod n$ (the "new position" of the bit x_i after $\sigma_j(x)$).

GHR is easy for quantum *SMP*

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Let $|1\rangle, \ldots, |n\rangle$ be an orthonormal basis for the space $\mathbb{R}^n$ of $\log n$ *qubits*.
- Let Alice and Bob send to the referee $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.
- Denote for $j, s \in [n]$: $u_j^s \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{\frac{\tau_s|_i + 1}{2}} \cdot |i\rangle \otimes |\sigma_j(i)\rangle \ \ (\in \mathbb{R}^{n^2})$, where $\sigma_j(i) \stackrel{\text{def}}{=} i + j \mod n$ (the "new position" of the bit x_i after $\sigma_j(x)$).
- Then $(u_j^s)_{j,s \in [n]}$ is an *orthonormal basis* for the space $\mathbb{R}^{n^2}$ of $2 \log n$ *qubits*: $(u_{j_1}^{s_1})^* \cdot u_{j_2}^{s_2} = 0$ if $[j_1 \neq j_2]$ or $[j_1 = j_2$ and $s_1 \neq s_2]$.
  That is, $\left\{u_j^s (u_j^s)^*\right\}_{j,s \in [n]}$ is a full set of pairwise-orthogonal projections in $\mathbb{R}^{n^2}$, corresponding to a *complete projective measurement of* $2 \log n$ *qubits*.

GHR is easy for quantum *SMP* (continued)

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Alice and Bob send to the referee $\log$ *n-qubit* states $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.
- For $j, s \in [n]$ and $u_j^s = \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{\frac{\tau_s|_i + 1}{2}} \cdot |i\rangle \otimes |\sigma_j(i)\rangle$, the family $\left\{u_j^s (u_j^s)^*\right\}_{j,s}$ is a *complete projective measurement* of $2 \log n$ *qubits*.

GHR is easy for quantum *SMP* (continued)

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Alice and Bob send to the referee $\log n$ *-qubit* states $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.
- For $j, s \in [n]$ and $u_j^s = \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{\frac{\tau_s|_i+1}{2}} \cdot |i\rangle \otimes |\sigma_j(i)\rangle$, the family $\left\{u_j^s (u_j^s)^*\right\}_{j,s}$ is a *complete projective measurement* of $2 \log n$ *qubits*.
- The referee applies it to the received $\alpha_x \otimes \beta_y$, and *the probability of the outcome "(j, s)"* is

$$\left|(\alpha_x \otimes \beta_y)^* \cdot u_j^s\right|^2 \sim \left(|\sigma_j(x \oplus \tau_s) \oplus y|_H - \frac{n}{2}\right)^2 = \left(|\rho_{j,s}(x) \oplus y|_H - \frac{n}{2}\right)^2.$$

GHR is easy for quantum *SMP* (continued)

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Alice and Bob send to the referee $\log$ *n-qubit* states $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.
- For $j, s \in [n]$ and $u_j^s = \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{\frac{\tau_s|_i + 1}{2}} \cdot |i\rangle \otimes |\sigma_j(i)\rangle$, the family $\left\{u_j^s (u_j^s)^*\right\}_{j,s}$ is a *complete projective measurement* of $2 \log n$ *qubits*.
- The referee applies it to the received $\alpha_x \otimes \beta_y$, and *the probability of the outcome* "(j, s)" is *proportional to* $\left(|\rho_{j,s}(x) \oplus y|_H - \frac{n}{2}\right)^2$.
- That is, our measurement "favours" the outcomes "(j, s)" that correspond to *"more biased"* $\rho_{j,s}(x) \oplus y$ *with respect to the Hamming weight*.

GHR is easy for quantum *SMP* (continued)

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

There is a *natural quantum procedure that "favours" correct answers*:

- Alice and Bob send to the referee $\log n$ *-qubit* states $\alpha_x \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{x_i} \cdot |i\rangle$ and $\beta_y \stackrel{\text{def}}{=} \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{y_i} \cdot |i\rangle$, respectively.
- For $j, s \in [n]$ and $u_j^s = \frac{1}{\sqrt{n}} \cdot \sum_{i=1}^{n} (-1)^{\frac{\tau_s|_i + 1}{2}} \cdot |i\rangle \otimes |\sigma_j(i)\rangle$, the family $\left\{u_j^s (u_j^s)^*\right\}_{j,s}$ is a *complete projective measurement* of $2 \log n$ *qubits*.
- The referee applies it to the received $\alpha_x \otimes \beta_y$, and *the probability of the outcome* "(j, s)" is *proportional to* $\left(|\rho_{j,s}(x) \oplus y|_H - \frac{n}{2}\right)^2$.
- That is, our measurement "favours" the outcomes "(j, s)" that correspond to *"more biased"* $\rho_{j,s}(x) \oplus y$ *with respect to the Hamming weight.*
- Repeating it $\log n$ times gives a $\mathcal{Q}^{\|}$*-protocol for GHR of cost* $O(\log^2 n)$.

GHR is hard for classical two-way ($\mathcal{R}$) – the proof idea

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

GHR is hard for classical two-way ($\mathcal{R}$) – the proof idea

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

- It is known (and intuitively clear) that *approximating* $|\mathcal{X} \oplus \mathcal{Y}|_H$ for uniformly-random $\mathcal{X}$ and $\mathcal{Y}$ *with accuracy* $\Theta\left(\sqrt{n}\right)$ is *hard for* $\mathcal{R}$.

GHR is hard for classical two-way ($\mathcal{R}$) – the proof idea

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

- It is known (and intuitively clear) that *approximating* $|\mathcal{X} \oplus \mathcal{Y}|_H$ for uniformly-random $\mathcal{X}$ and $\mathcal{Y}$ *with accuracy* $\Theta(\sqrt{n})$ is *hard for* $\mathcal{R}$.
- We sharpen this statement and show that if Π *is an efficient protocol in* $\mathcal{R}$, then *the distribution of* $|\rho_{j,s}(\mathcal{X}) \oplus \mathcal{Y}|_H$ is very similar in the cases *when the distribution of* $(\mathcal{X}, \mathcal{Y})$ *is uniform* and *when it is conditioned on a "typpical" transcript of* Π (and this holds for each j and s).

GHR is hard for classical two-way ($\mathcal{R}$) – the proof idea

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x, y)$ if, assuming $\aleph(x, y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

- It is known (and intuitively clear) that *approximating* $|\mathcal{X} \oplus \mathcal{Y}|_H$ for uniformly-random $\mathcal{X}$ and $\mathcal{Y}$ *with accuracy* $\Theta(\sqrt{n})$ is *hard for* $\mathcal{R}$.
- We sharpen this statement and show that if Π *is an efficient protocol in* $\mathcal{R}$, then *the distribution of* $|\rho_{j,s}(\mathcal{X}) \oplus \mathcal{Y}|_H$ is very similar in the cases *when the distribution of* $(\mathcal{X}, \mathcal{Y})$ *is uniform* and *when it is conditioned on a "typpical" transcript of* Π (and this holds for each j and s).
- This suffices to show that *the* $\mathcal{R}$*-complexity of GHR is* $\Omega(n^{1/3})$.

GHR is hard for classical two-way ($\mathcal{R}$) – the proof idea

Recall: $x, y \in \{0,1\}^n$, $\rho_{j,s}(x) = \sigma_j(\tau_s \oplus x)$ and $((j_1, s_1), \ldots, (j_{\log n}, s_{\log n}))$ is a *valid answer* to $GHR(x,y)$ if, assuming $\aleph(x,y)$,

$$\left|\left\{i : |\rho_{j_i,s_i}(x) \oplus y|_H \notin \left[\frac{n}{2} - \frac{\sqrt{n}}{2}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right]\right\}\right| \geq \frac{\log n}{2}.$$

- It is known (and intuitively clear) that *approximating* $|\mathcal{X} \oplus \mathcal{Y}|_H$ for uniformly-random $\mathcal{X}$ and $\mathcal{Y}$ *with accuracy* $\Theta\left(\sqrt{n}\right)$ is *hard for* $\mathcal{R}$.
- We sharpen this statement and show that if Π *is an efficient protocol in* $\mathcal{R}$, then *the distribution of* $|\rho_{j,s}(\mathcal{X}) \oplus \mathcal{Y}|_H$ is very similar in the cases *when the distribution of* $(\mathcal{X}, \mathcal{Y})$ *is uniform* and *when it is conditioned on a "typpical" transcript of* Π (and this holds for each j and s).
- This suffices to show that *the* $\mathcal{R}$*-complexity of GHR is* $\Omega\left(n^{1/3}\right)$.

That is, *GHR is easy for* $\mathcal{Q}^{\|}$ (complexity $O\left(\log^2 n\right)$) but *hard for* $\mathcal{R}$ (complexity $\Omega\left(n^{1/3}\right)$).

Відкриті проблеми

Залишається багато цікавих питань стосовно квантової комунікаційної складності, наприклад:

Відкриті проблеми

Залишається багато цікавих питань стосовно квантової комунікаційної складності, наприклад:

- Чи може взагалі квантова комунікаційна модель мати якісну перевагу над своїм класичним аналогом (сильнішим за $\mathcal{R}^{\|}$) відносно *всюди визначені (BB) функції*?
  Інакше кажучи, *наскільки сильні зразки переваги* квантової комунікації може дати цей "найобмеженіший" тип задач?

Відкриті проблеми

Залишається багато цікавих питань стосовно квантової комунікаційної складності, наприклад:

- Чи може взагалі квантова комунікаційна модель мати якісну перевагу над своїм класичним аналогом (сильнішим за $\mathcal{R}^{\|}$) відносно *всюди визначені (ВВ) функції*?
  Інакше кажучи, *наскільки сильні зразки переваги* квантової комунікації може дати цей "найобмеженіший" тип задач?
- Чи може $\mathcal{Q}^{\|}$ бути якісно сильнішою за $\mathcal{R}$ у випадку *функції* (хоча б ЧВ)?
  Інакше кажучи, *"наскільки необмеженим" має бути тим комунікаційної задачі*, що демонструє найсильніший з відомих на сьогодні приклад якісною переваги квантової комунікації?