Distributed Computing with Quantum Ressources and Beyond

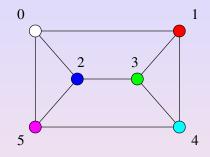
Cyril Gavoille

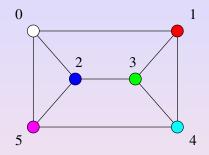
Describerte LaBRI, University of Bordeaux

Complexity, Algorithms, Automata and Logic Meet (CAALM) Chennai Mathematical Institute January 22, 2019

Agenda

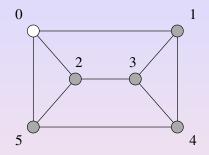
- **1** The Coloring Problem
- Oistributed Computing
- **3** Quantum Information
- Beyond Quantum



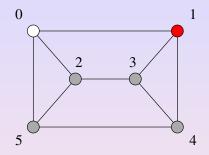


Sequentiel greedy algorithm: First Free

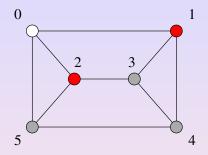
For each node u, in any order, color u with the smallest available color in the palette $\frac{0}{2} = \frac{1}{2} = \frac{3}{2} = \frac{1}{2}$



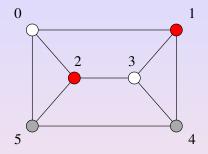
Sequentiel greedy algorithm: First Free



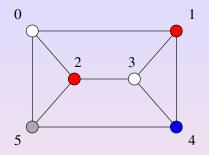
Sequentiel greedy algorithm: First Free



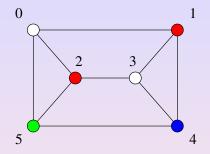
Sequentiel greedy algorithm: First Free



Sequentiel greedy algorithm: First Free



Sequentiel greedy algorithm: First Free



Sequentiel greedy algorithm: FirstFree

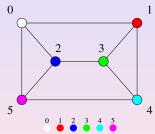
For each node u, in any order, color u with the smallest available color in the palette $\overset{0}{\bullet} \overset{1}{\bullet} \overset{2}{\bullet} \overset{3}{\bullet} \overset{4}{\bullet} \overset{5}{\bullet}$

"Few" means at most $\Delta + 1$ colors ($\Delta = \max \text{ degree}$) [Ordering 0, 2, 5, 4, 3, 1 would give $\chi = 3$ colors]

Distributed Graph Coloring

The distributed system is the graph it-self.

 $\mbox{Goal.}$ To produce a $(\Delta+1)\mbox{-coloring}$ by inspecting neighborhoods only.

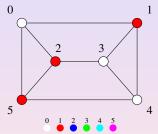


Running in parallel First Free...

Distributed Graph Coloring

The distributed system is the graph it-self.

Goal. To produce a $(\Delta + 1)$ -coloring by inspecting neighborhoods only.

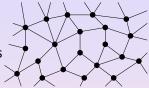


Running in parallel FirstFree... does not work. We would like they don't act at the same round. Works if they have different color!

The LOCAL Model (focuses on locality of a task)

- Nodes have IDs
- Nodes run in synchronous rounds
- Communication between neighbors
- No message size limits
- No local computational power limits
- No failures

Complexity measure. The number of rounds

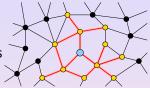


The LOCAL Model (focuses on locality of a task)

- Nodes have IDs
- Nodes run in synchronous rounds
- Communication between neighbors
- No message size limits
- No local computational power limits
- No failures

Complexity measure. The number of rounds

A task can be solved in k rounds iff nodes can decide their output by inspecting their distance-k neighborhood.



Distributed $(\Delta + 1)$ -Coloring

Challenge. Design a parallel version of a typically greedy algorithm. A fundamental and toy problem, likewise a drosophilia fly of biologists.



Distributed $(\Delta + 1)$ -Coloring

Challenge. Design a parallel version of a typically greedy algorithm. A fundamental and toy problem, likewise a drosophilia fly of biologists.



Best known bounds (#rounds)



• $\frac{1}{2}\log^* n$

•
$$O(\sqrt{\Delta \log^5 \Delta}) + \log^* n$$

• $O(\sqrt{\log \Delta}) + 2O(\sqrt{\log \log n})$

 $O(\sqrt{\log \Delta})$ +

[STOC'92] [FOCS'87]

[FOCS'16] (rand.) [STOC'16]

$$\log^* n = \min\left\{i \in \mathbb{N} : \log^{(i)} n \leqslant 1\right\}$$

Beyond the LOCAL Model

Goal. Study the locality of a problem when nodes have access to exotic ressources, like entangled qubits or others.

Beyond the LOCAL Model

Goal. Study the locality of a problem when nodes have access to exotic ressources, like entangled qubits or others.

Extensions of the LOCAL model:

- Shared-randomness ressources
- 2 Quantum ressources
- 3 Any ressource and mechanism preserving physical locality

Beyond the LOCAL Model

Goal. Study the locality of a problem when nodes have access to exotic ressources, like entangled qubits or others.

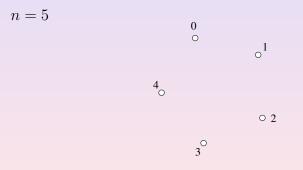
Extensions of the LOCAL model:

- Shared-randomness ressources
- 2 Quantum ressources
- 3 Any ressource and mechanism preserving physical locality

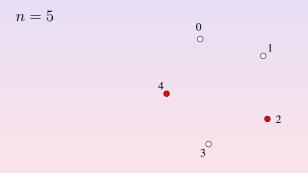
Fact. Shared-randomness does not help for 3-coloring a cycle, $\Omega(\log^* n)$ still holds. Unknown for quantum ressources.

There are proof-of-concept problems showing that it may help.

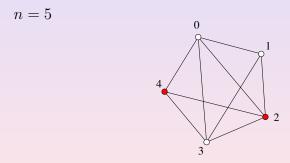
Task. Select in 0 rounds two adjacent nodes in G isomorphic to $K_n \setminus \{e\}$. To win, exactly two adjacent nodes must output **select**, the others **unselect**.

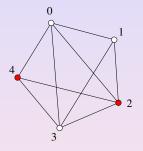


Task. Select in 0 rounds two adjacent nodes in G isomorphic to $K_n \setminus \{e\}$. To win, exactly two adjacent nodes must output **select**, the others **unselect**.



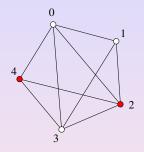
Task. Select in 0 rounds two adjacent nodes in G isomorphic to $K_n \setminus \{e\}$. To win, exactly two adjacent nodes must output **select**, the others **unselect**.





Cannot be solved in the classical LOCAL model with Pr > 1/e.

[One can tends to $1/e \approx 36\%$ by always selecting node with ID= 0 and each other with Pr = (n-2)/(n-1), if $n \ge 6$]



With shared-randomness, each node can select any edge of K_n uniformly at random in a coordinated manner.

$$\Pr(\mathsf{win}) = 1 - 1 / \binom{n}{2} = 1 - o(1)$$

Quantum Extension



Nodes may share arbitrary entangled states (before inputs come) ... use quantum communication channels with teleportation effects and others.

To understand why quantum extensions is strictly stronger than shared-randomness extensions, we need to introduce quantum information background ...

Quantum Physics (for computer scientists)



Two fundamental principles in physics:

- Causality: Causes preceed consequences.
- Locality: No instantaneously and distant interactions.

Two fundamental principles in physics:

- Causality: Causes preceed consequences.
- Locality: No instantaneously and distant interactions.

Reproducible experiments of Alain Aspect in '82 show that one of the two principles (at least) does not hold ... Bell's inequalities are violated.

Causality & Locality

+ Quantum effects/non-locality: a quantum particle (the support of information) can be in several places at the same time (superposition) ... Really.

Causality & Locality

+ Quantum effects/non-locality: a quantum particle (the support of information) can be in several places at the same time (superposition) ... Really.

- Unlike relativity theory, quantum physics do not logically follows from easy-to-validate axioms, like the invariance principle and causality.

BTW, invariance (laws are the same under any coordinates axis) and causality imply an upper bound speed limit for light.

Deterministic bit B: represented by a value $B \in \{0, 1\}$.

Deterministic bit B: represented by a value $B \in \{0, 1\}$.

Probabilistic bit P: represented by a real vector $\begin{pmatrix} p \\ a \end{pmatrix}$

- p = probability to get 0
- q =probability to get 1

Required: p + q = 1

Deterministic bit B: represented by a value $\mathbf{B} \in \{0, 1\}$.

Probabilistic bit P: represented by a real vector $\begin{pmatrix} p \\ a \end{pmatrix}$

- p = probability to get 0
- q =probability to get 1

Required: p + q = 1

Interpret vector
$$\begin{pmatrix} 1\\ 0 \end{pmatrix}$$
 as the value 0, and $\begin{pmatrix} 0\\ 1 \end{pmatrix}$ as 1. Then

$$\mathbf{P} = p \begin{pmatrix} 1\\ 0 \end{pmatrix} + q \begin{pmatrix} 0\\ 1 \end{pmatrix} = \begin{pmatrix} p\\ q \end{pmatrix}$$

Quantum bit Q: represented by a complexe vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

- $|\alpha|^2 = \text{probability to get } \mathbf{0}$
- $|\beta|^2 = \text{probability to get } \mathbf{1}$

Required: $|\alpha|^2 + |\beta|^2 = 1$

Quantum bit Q: represented by a complexe vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

- $|\alpha|^2 = \text{probability to get } \mathbf{0}$
- $|\beta|^2 = \text{probability to get } \mathbf{1}$

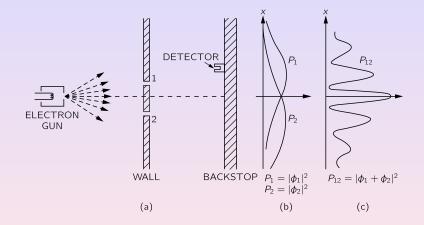
Required: $|\alpha|^2 + |\beta|^2 = 1$

Interpret vector
$$\begin{pmatrix} 1\\ 0 \end{pmatrix}$$
 as the value **0**, and $\begin{pmatrix} 0\\ 1 \end{pmatrix}$ as **1**. Then

$$\mathbf{Q} = \alpha \begin{pmatrix} 1\\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0\\ 1 \end{pmatrix} = \begin{pmatrix} \alpha\\ \beta \end{pmatrix}$$

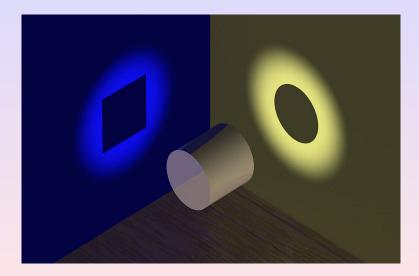
Implemented by a physical particle (photon, electron, atome). The **mesure** of a qubit is a physical measurement of an **observable**, a property like: polarization, spin, electrical charge, energy level, speed, position, impulsion, ...

Superposition & Interference



Superposition even for a single particle ...

Reality?



Entanglement of Qubit Systems

A system of two independent probabilist bits $\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}$ and $\begin{pmatrix} p_2 \\ q_2 \end{pmatrix}$ represented by a tensor product.

$$\begin{pmatrix} p_1 \\ q_1 \end{pmatrix} \otimes \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} = \begin{pmatrix} p_1 \cdot \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \\ q_1 \cdot \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} p_1 p_2 \\ p_1 q_2 \\ q_1 p_2 \\ q_1 p_2 \\ q_1 q_2 \end{pmatrix}$$
$$= p_1 p_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + p_1 q_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + q_1 p_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + q_1 q_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + q_1 q_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Entanglement of Qubit Systems

A system (A, B) composed of two qubits represented as linear combinaisons of four unit vectors:

$$(A,B) = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = c_{00} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + c_{01} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + c_{10} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + c_{11} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

where $c_{ij} \in \mathbb{C}$ and $\sum_{ij} |c_{ij}|^2 = 1$, the probability to observe A = i et B = j being controlled by $|c_{ij}|^2$.

Entangled vs. Separable States

The state of a system (A, B) is separable if $(A, B) = A \otimes B$. Otherwise it is entangled.

$$(A,B) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix}$$

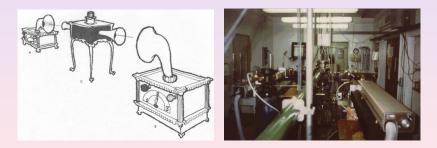
Operators

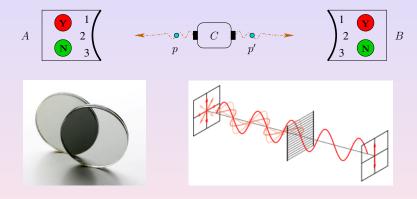
The state of a system S of n qubits is denoted $|S\rangle$ which is a vector in \mathbb{H}^{2^n} . Operations on state vector is a **reversible** unit matrix of $\mathbb{H}^{2^n \times 2^n}$.

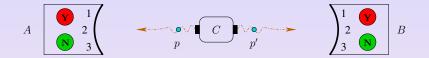
For n = 1. $NOT := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad NOT \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $R(\theta) := \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ $\sqrt{\text{NOT}} := \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}, \quad \sqrt{\text{NOT}} \cdot \sqrt{\text{NOT}} = \text{NOT}$

On Bell's Inequalities

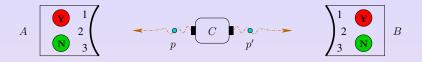
Using a *Gedankenexperiment* invented by David Bohm (1951), John S. Bell (1964) showed that the **nonexistence of properties before measurement** is a direct consequence of the quantitative numerical predictions of the quantum theory. Alain Aspect (1982) showed that the quantum-theoretic predictions were indeed obeyed.







12GR	32RG	32GR	22RR	33RR	12RG	22GG	13RG	21RG
22GG	11GG	31RG	22RR	21RG	21GG	21GR	11GG	13GR
11GG	31RG	32RG	21GR	31GR	31RG	12GR	23RG	11RR
21GR	13GR	13RG	33GG	21RR	12RG	33RR	23RG	23GR
33GG	33RR	12RR	21RG	31GR	32GR	23RR	13GG	23GG
33RR	12GR	12RG	31GG	33GG	13GG	32GR	32RR	23RG
11RR	31GR	22RR	11RR	23GR	23GR	22GG	13RR	33GG
22GG	11GG	12GR	32RG	32GG	31RR	13RG	22RR	11RR



12GR	32RG	32GR	22RR	33RR	12RG	22GG	13RG	21RG
22GG	11GG	31RG	22RR	21RG	21GG	21GR	11GG	13GR
11GG	31RG	32RG	21GR	31GR	31RG	12GR	23RG	11RR
21GR	13GR	13RG	33GG	21RR	12RG	33RR	23RG	23GR
33GG	33RR	12RR	21RG	31GR	32GR	23RR	13GG	23GG
33RR	12GR	12RG	31GG	33GG	13GG	32GR	32RR	23RG
11RR	31GR	22RR	11RR	23GR	23GR	22GG	13RR	33GG
22GG	11GG	12GR	32RG	32GG	31RR	13RG	22RR	11RR

(U) Uniformity. If we look only flashs, results are uniform random(C) Correlation. If same detector positions, then flash same color



(U) Uniformity. If we look only flashs, results are uniform random(C) Correlation. If same detector positions, then flash same color

Hypothesis. What is measured by detectors is an intrinsic property of the particles that is fixed before measurement. (Fixed at the creation in C, or along their travel to A or B, but before fixing selecting positions.)



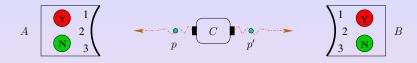
Hypothesis. What is measured by detectors is an intrinsic property of the particles that is fixed before measurement.

For type RGR, same flashs for positions 11, 22, 33 or 13, 31 (and \neq flashs for 12, 21, 23, 32). Positions are selected indep. uniformly at random (1/9 each pair), so we should obtained same flashs 5/9 > 55% of the time.



Hypothesis. What is measured by detectors is an intrinsic property of the particles that is fixed before measurement.

More generally, for types with twice the same letter (RGR, RRG, RGR, GRR, GGR, GRG and RGG) we should observe same flashs 55% of the time. For types RRR and GGG, it should occur 100% of the time.



Hypothesis. What is measured by detectors is an intrinsic property of the particles that is fixed before measurement.

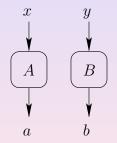
More generally, for types with twice the same letter (RGR, RRG, RGR, GRR, GGR, GRG and RGG) we should observe same flashs 55% of the time. For types RRR and GGG, it should occur 100% of the time.

Whatever the type distribution, detectors should flash the same color at least 55% of the time, contradicting **(U)**.

Property **does not exist** before measurement

The CHSH Game: $a \oplus b = x \wedge y$

Input: $x, y \in \{0, 1\}$ **Output:** $a, b \in \{0, 1\}$



The CHSH Game: $a \oplus b = x \wedge y$

(1) No deterministic strategies allow Alice & Bob to win.

$$a(0) \oplus b(0) = 0 \land 0 = 0$$

$$a(0) \oplus b(1) = 0 \land 1 = 0$$

$$a(1) \oplus b(0) = 1 \land 0 = 0$$

$$a(1) \oplus b(1) = 1 \land 1 = 1$$

(2) If Alice & Bob share random bits, then they have a strategy to win 75% of the times, and no probabilistic algorithm can do better.

x	y	$x \wedge y$	0	1	x	$\neg x$	y	$\neg y$	$x \oplus y$	$\neg x \oplus y$	success probability
0	0	0	p_1	0	p_3	0	p_5	0	p_7	0	$P_{00} = p_1 + p_3 + p_5 + p_7$
0	1	0	p_1	0	0	p_4	p_5	0	0	p_8	$P_{01} = p_1 + p_4 + p_5 + p_8$
1	0	0	p_1	0	p_3	0	0	p_6	0	p_8	$P_{10} = p_1 + p_3 + p_6 + p_8$
1	1	1	0	p_2	p_3	0	p_5	0	0	p_8	$P_{11} = p_2 + p_3 + p_5 + p_8$

 $\min \left\{ P_{00}, P_{01}, P_{10}, P_{11} \right\} \leqslant 3/4$

because $S = P_{00} + P_{01} + P_{10} + P_{11} =$ $3p_1 + p_2 + 3p_3 + p_4 + 3p_5 + p_6 + p_7 + p_8 \leq 3 \cdot (p_1 + \dots + p_8) \leq 3.$ (3) If Alice & Bob have qubits, then they have a strategy to win $\cos^2(\pi/8) > 85\%$ of the times, and no quantum algorithm can do better.

$$|A,B\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix}$$

Alice applies a rotation $R(\theta)$ with $\theta = -\pi/16$ if x = 0 and $3\pi/16$ is x = 1. Similarly for Bob.

(1) No deterministic strategies allow Alice & Bob to win.

(2) If Alice & Bob share random bits, then they have a strategy to win 75% of the times, and no probabilistic algorithm can do better.

(3) If Alice & Bob have qubits, then they have a strategy to win $\cos^2(\pi/8) > 85\%$ of the times, and no quantum algorithm can do better.

The φ -LOCAL Model (the ultimate non-signalling local model?)



Aim

+ A weaker model than the quantum extension of the LOCAL model for a better understanding of the absolute limits of any conceivable extensions of the LOCAL model by any non-signalling physical theory (preserving causality principle).

Aim

- + A weaker model than the quantum extension of the LOCAL model for a better understanding of the absolute limits of any conceivable extensions of the LOCAL model by any non-signalling physical theory (preserving causality principle).
- + A simple combinatorial model avoiding linear algebra in Hilbert space.

Aim

- + A weaker model than the quantum extension of the LOCAL model for a better understanding of the absolute limits of any conceivable extensions of the LOCAL model by any non-signalling physical theory (preserving causality principle).
- + A simple combinatorial model avoiding linear algebra in Hilbert space.
- Does not give concrete distributed algorithms because instructions with new physics may do not exist yet.

The Physical Locality: the φ -LOCAL Model

Thesis. Locality is violated if and only if, based on the available output data, we can conclusively verify that after k rounds some subset S of nodes was affected by input data of G initially localized outside its view.

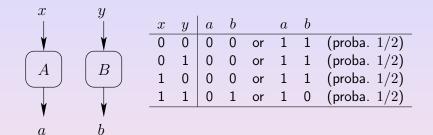
In the φ -LOCAL model, we allow any kind of correlation (possibly non-local) in the output distribution that does not violate locality. It allows **non-signalling** distributions only.

If A, B are nodes at distance more than k, then for an entry (x, y), the output (a, b) must verify the **non-signalling** property:

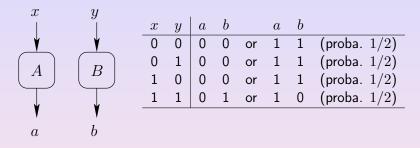
$$\Pr(a|x,y) =_{\text{def}} \sum_{b} \Pr(a,b|x,y) = \Pr(a|x)$$

$$\Pr(b|x,y) =_{\text{def}} \sum_{a} \Pr(a,b|x,y) = \Pr(b|y) .$$

Non-Signalling Distribution



Non-Signalling Distribution



 $\mathsf{NB}: a \oplus b = x \land y$

(4) There is a distribution in the φ -LOCAL model with k = 0 round that allows Alice & Bob to win the CHSH game 100% of the time.

The best currently known round lower bounds for many distributed problems, such as **Maximal Independent Set** (MIS) in general graphs, cannot be broken with quantum or non-signalling LOCAL extensions.

The best currently known round lower bounds for many distributed problems, such as **Maximal Independent Set** (MIS) in general graphs, cannot be broken with quantum or non-signalling LOCAL extensions.

E.g., MIS requires $\Omega(\sqrt{\log n/\log\log n})$ rounds in general graphs in the $\varphi\text{-LOCAL}$ model.

The best currently known round lower bounds for many distributed problems, such as **Maximal Independent Set** (MIS) in general graphs, cannot be broken with quantum or non-signalling LOCAL extensions.

E.g., MIS requires $\Omega(\sqrt{\log n / \log \log n})$ rounds in general graphs in the φ -LOCAL model.

The $\Omega(\log^* n)$ lower bound for 3-coloring a ring (or MIS in a path) is **not** a view based argument.

 \bullet 2-coloring a ring requires $\lceil n/4\rceil$ rounds, and this is tight.

- 2-coloring a ring requires $\lceil n/4 \rceil$ rounds, and this is tight.
- 2-coloring a path requires $\lceil n/3 \rceil$ rounds, and this is tight.

- $\bullet~2\text{-coloring}$ a ring requires $\lceil n/4\rceil$ rounds, and this is tight.
- 2-coloring a path requires $\lceil n/3\rceil$ rounds, and this is tight.
- Computing an MIS for a path requires at least two rounds, and three rounds are sufficient.

- $\bullet~2\text{-coloring}$ a ring requires $\lceil n/4\rceil$ rounds, and this is tight.
- 2-coloring a path requires $\lceil n/3 \rceil$ rounds, and this is tight.
- Computing an MIS for a path requires at least two rounds, and three rounds are sufficient.
- [Holroyd-Ligget'16] have constructed a stationary 1-dependent distribution for 4-coloring a path.
 ⇒ 4-coloring can be done in one half-round, and 3-coloring in one round.

- $\bullet~2\text{-coloring}$ a ring requires $\lceil n/4\rceil$ rounds, and this is tight.
- 2-coloring a path requires $\lceil n/3 \rceil$ rounds, and this is tight.
- Computing an MIS for a path requires at least two rounds, and three rounds are sufficient.
- [Holroyd-Ligget'16] have constructed a stationary 1-dependent distribution for 4-coloring a path.
 ⇒ 4-coloring can be done in one half-round, and 3-coloring in one round.
- 3-coloring a path cannot be done in one half-round.

Thank you!