Stabilizing Consensus with Many Opinions

Emanuele Natale*

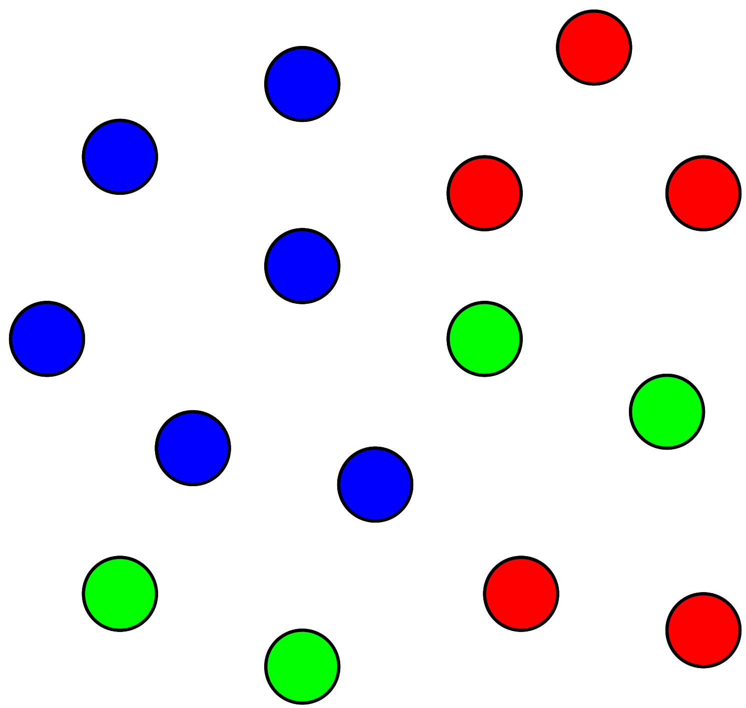
joint work with
Luca Becchetti*, Andrea Clementi†,
Francesco Pasquale* and Luca Trevisan‡

† Sapienza Università di Roma
* Università degli Studi di Roma Tor Vergata
‡ Berkeley University of California

ACM-SIAM Symposium on Discrete Algorithms
January 10-12, 2016
Crystal Gateway Marriott
Arlington, Virginia, USA

Stabilizing Almost-Consensus

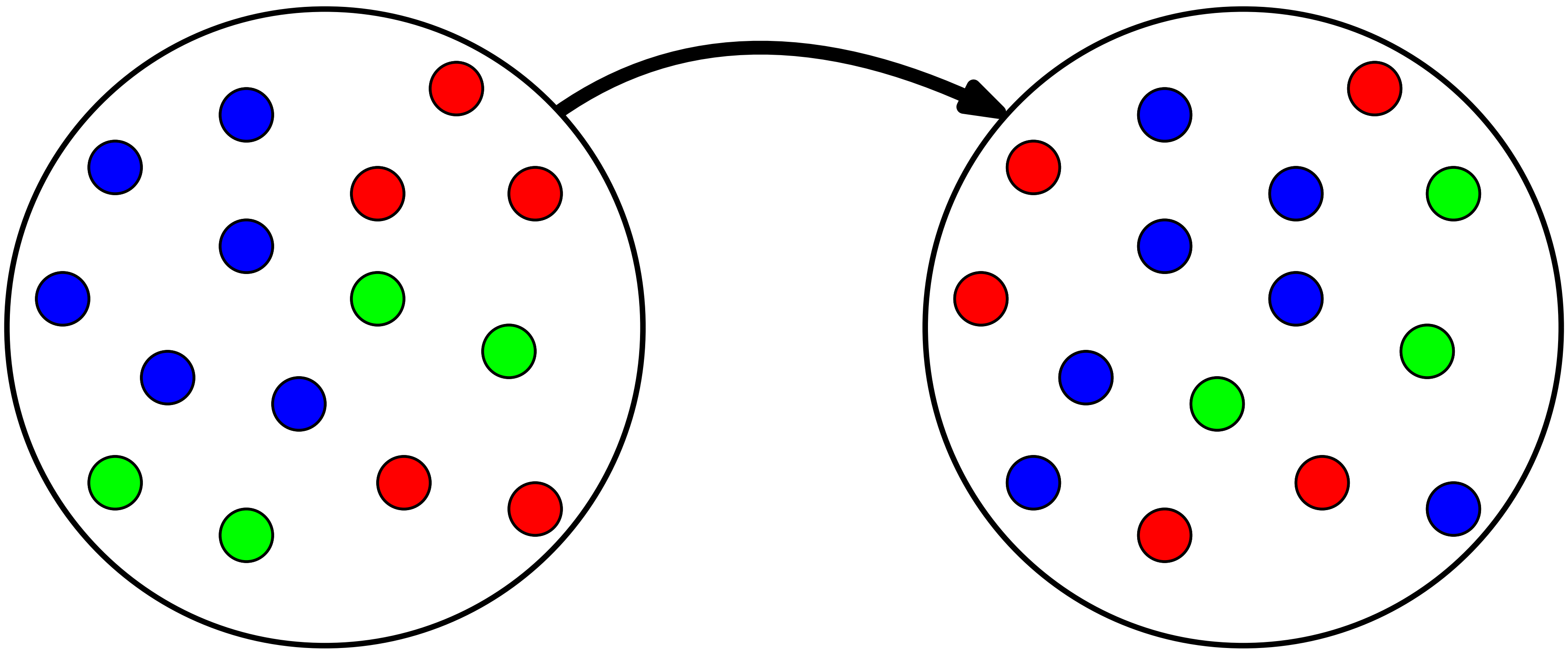
A set of nodes each having one color out of a set Σ.



Initial colors are called *valid*.

Stabilizing Almost-Consensus

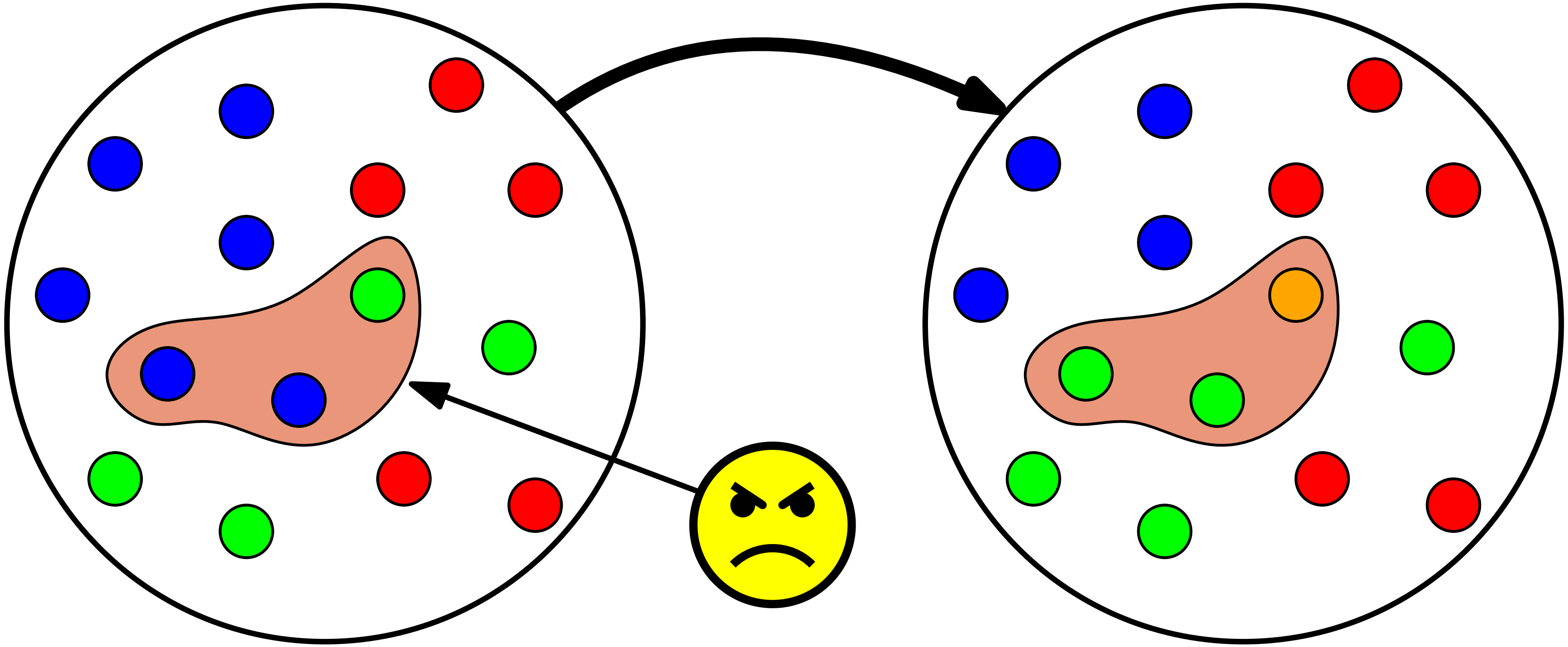
At the start of each round, nodes uptate their color,



according to the given communication model and protocol.

Stabilizing Almost-Consensus

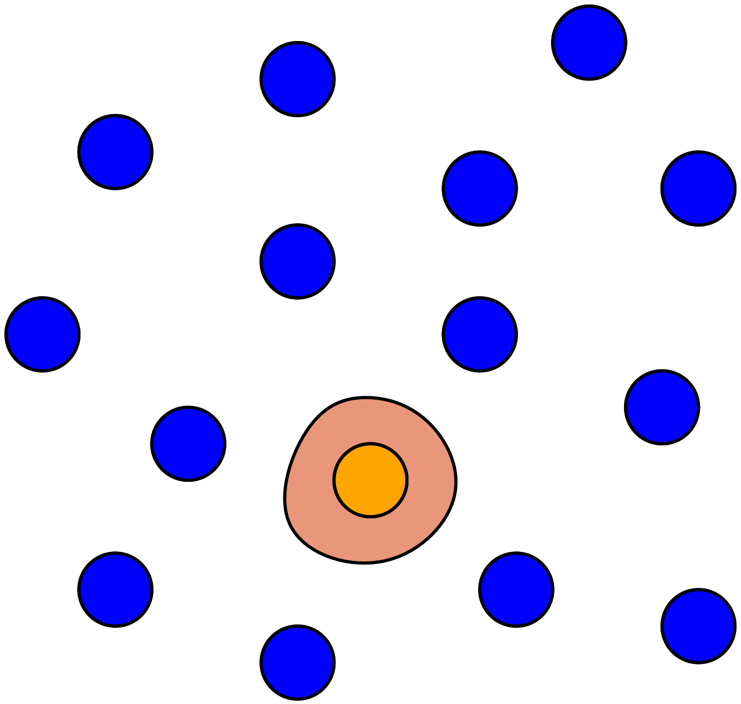
At the end of each round, an F-dynamic adversary can change the color of F nodes,



possibly chosing different subsets of nodes over different rounds.

Stabilizing Almost-Consensus

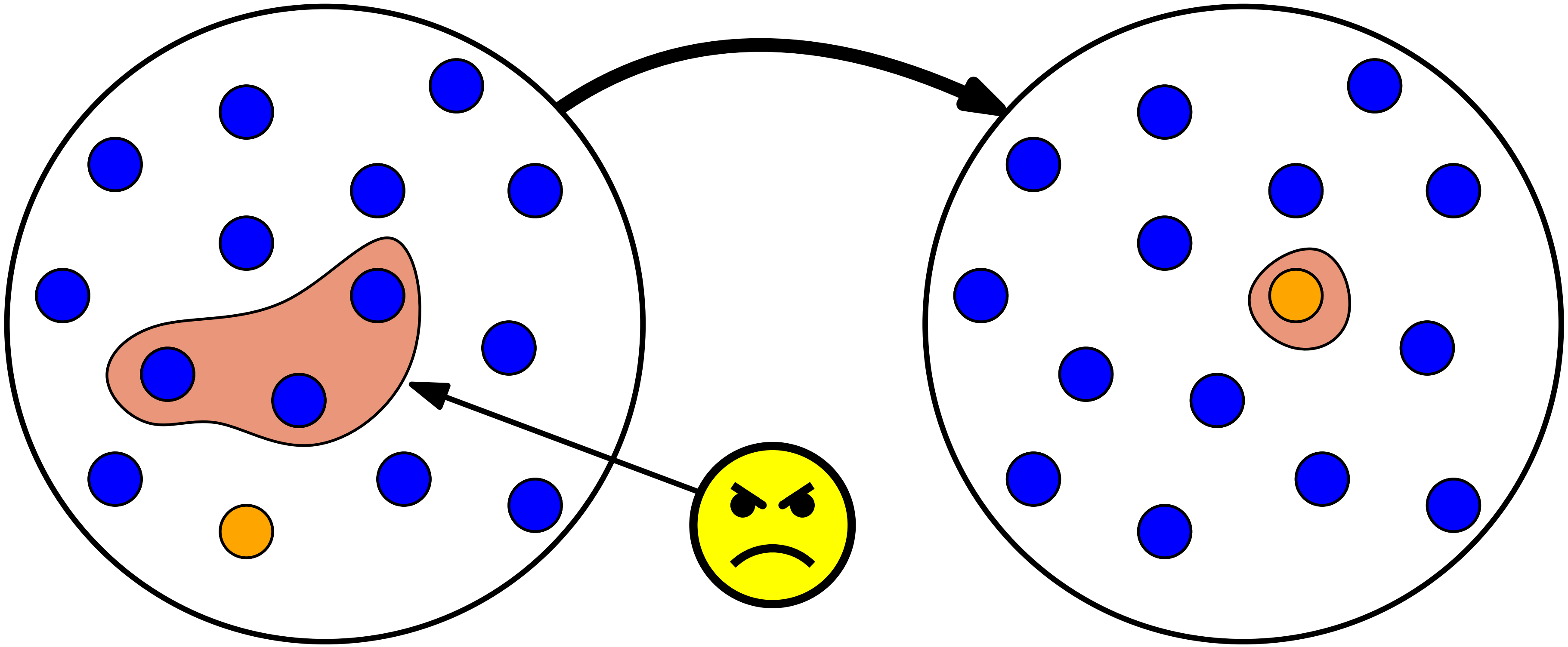
Except for a small number of nodes
we want to reach consensus (almost consensus),



on any valid color (almost validity),

Stabilizing Almost-Consensus

Almost-consensus has to be preserved for any poly(n) rounds,



even if the adversary changes colors at each round (almost stability).

Stabilizing Almost-Consensus

A *stabilizing almost-consensus* protocol guarantees that, w.h.p., for some $\gamma < 1$, from any initial conf., in a finite number of rounds, the system reaches a set of conf.s where $n - \mathcal{O}(n^{\gamma})$ nodes

- hold the same color (*almost consensus*),
- the color was in the initial conf. (*almost validity*),
- and the convergence hold for any poly(n) rounds (*almost stability*).

Stabilizing Almost-Consensus

A *stabilizing almost-consensus* protocol guarantees that, w.h.p., for some $\gamma < 1$, from any initial conf., in a finite number of rounds, the system reaches a set of conf.s where $n - \mathcal{O}(n^\gamma)$ nodes

- hold the same color (*almost consensus*),
- the color was in the initial conf. (*almost validity*),
- and the convergence hold for any poly(n) rounds (*almost stability*).

Cf. classical byzantine agreement:
agreement, validity and termination.

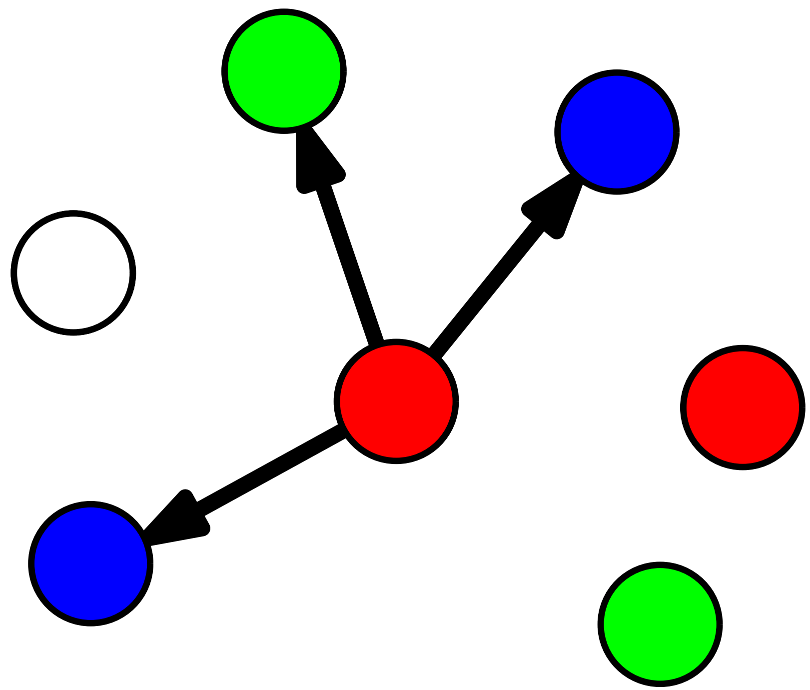
The Setting

Communication model. Uniform Gossip model: Each node in one round can communicate with one node chosen u.a.r.

Protocol constraints. *simple* rule (dynamics): Anonymous, $O(\log |\Sigma|)$ local memory and message size, counters of non-constant length, ...

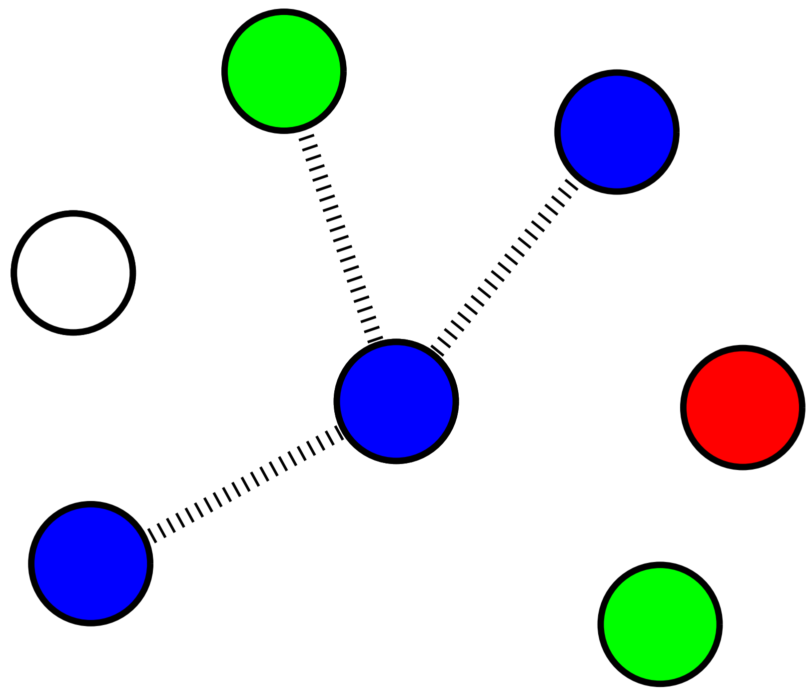
Motivations. Biological systems, chemical reaction networks, social networks, sensor networks.

Previous Work: 3-Median Dynamics



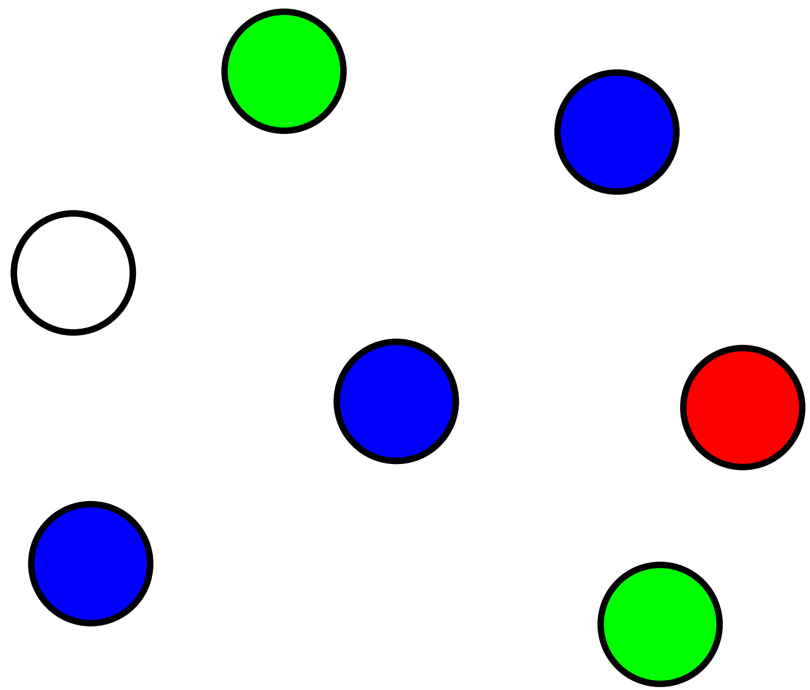
Each node observes the color of three other nodes chosen u.a.r....

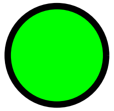
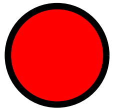
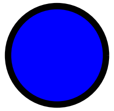
Previous Work: 3-Median Dynamics



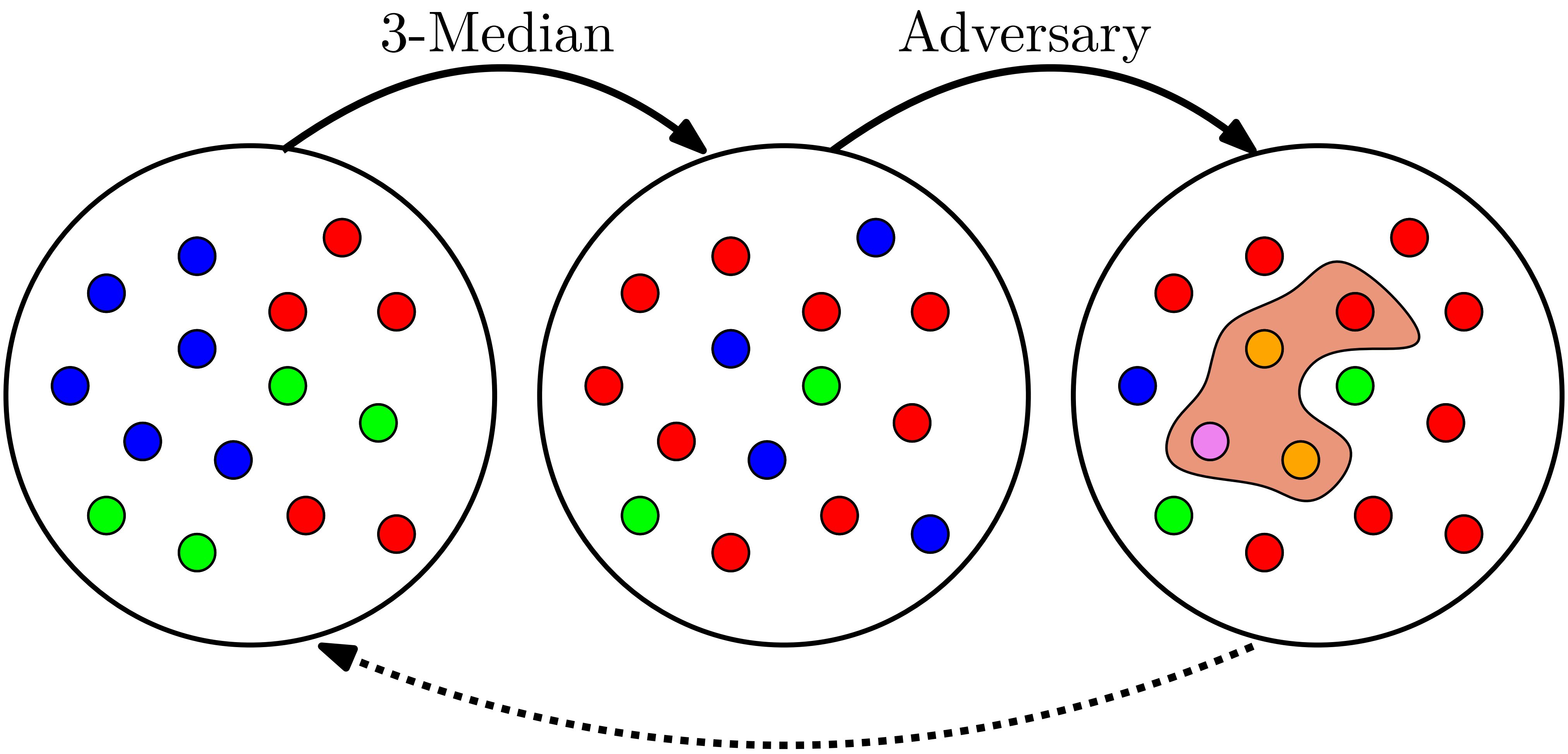
...and changes its color according to the median of these three...

Previous Work: 3-Median Dynamics



Colors are totally ordered: ...<  <  <  <...

The 3-Median Process



Almost consensus? Almost validity? Almost stability?

3-Median Dynamics

Theorem (Doerr, Goldberg, Minder, Sauerwald, Scheideler '11). For any $\sqrt{n}$-bounded adversary, the **3-median** computes an almost stable value between the $(n/2 - c\sqrt{nlogn})$-largest and the $(n/2 + c\sqrt{nlogn})$- largest of the initial values, in $\mathcal{O}(\log k \cdot \log \log n + \log n)$ rounds w.h.p.

3-Median Dynamics

Theorem (Doerr, Goldberg, Minder, Sauerwald, Scheideler '11). For any $\sqrt{n}$-bounded adversary, the **3-median** computes an almost stable value between the $(n/2 - c\sqrt{nlogn})$-largest and the $(n/2 + c\sqrt{nlogn})$- largest of the initial values, in $\mathcal{O}(\log k \cdot \log\log n + \log n)$ rounds w.h.p.

Does 3-median guarantee Stabilizing Almost Consensus?

- Almost consensus ✓
- Almost validity
- Almost stability

3-Median Dynamics

Theorem (Doerr, Goldberg, Minder, Sauerwald, Scheideler '11). For any $\sqrt{n}$-bounded adversary, the **3-median** computes an almost stable value between the $(n/2 - c\sqrt{nlogn})$-largest and the $(n/2 + c\sqrt{nlogn})$- largest of the initial values, in $\mathcal{O}(\log k \cdot \log\log n + \log n)$ rounds w.h.p.

Does 3-median guarantee Stabilizing Almost Consensus?

- Almost consensus ✓
- Almost validity
- Almost stability ✓

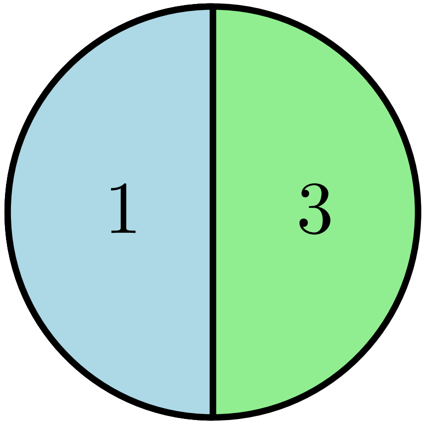
3-Median Dynamics

Theorem (Doerr, Goldberg, Minder, Sauerwald, Scheideler '11). For any $\sqrt{n}$-bounded adversary, the **3-median** computes an almost stable value between the $(n/2 - c\sqrt{nlogn})$-largest and the $(n/2 + c\sqrt{nlogn})$- largest of the initial values, in $\mathcal{O}(\log k \cdot \log\log n + \log n)$ rounds w.h.p.

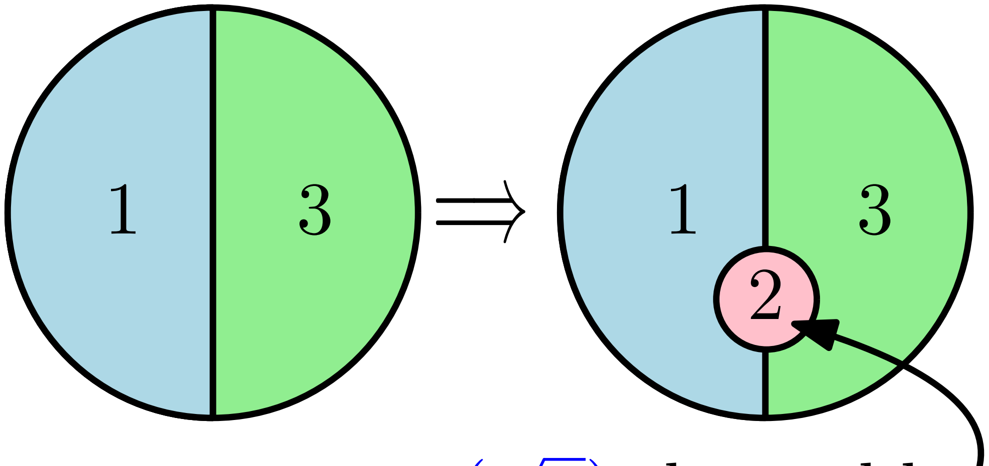
Does 3-median guarantee Stabilizing Almost Consensus?

- Almost consensus ✓
- Almost validity?
- Almost stability ✓

3-Median Dynamics



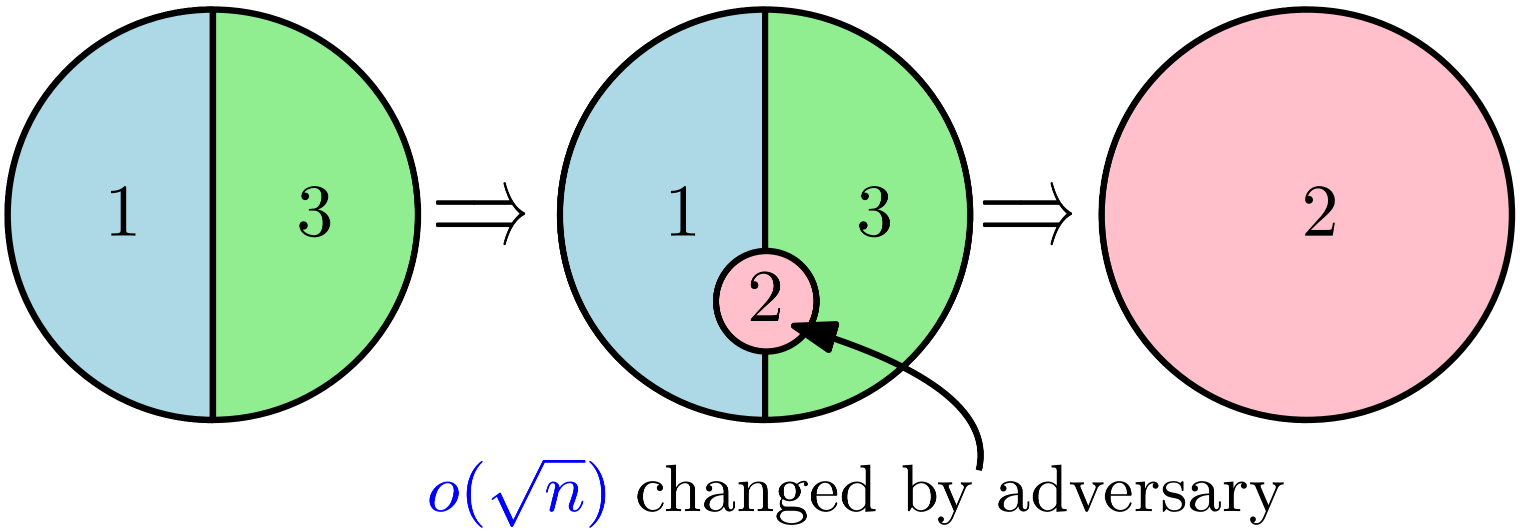
3-Median Dynamics



$o(\sqrt{n})$ changed by adversary

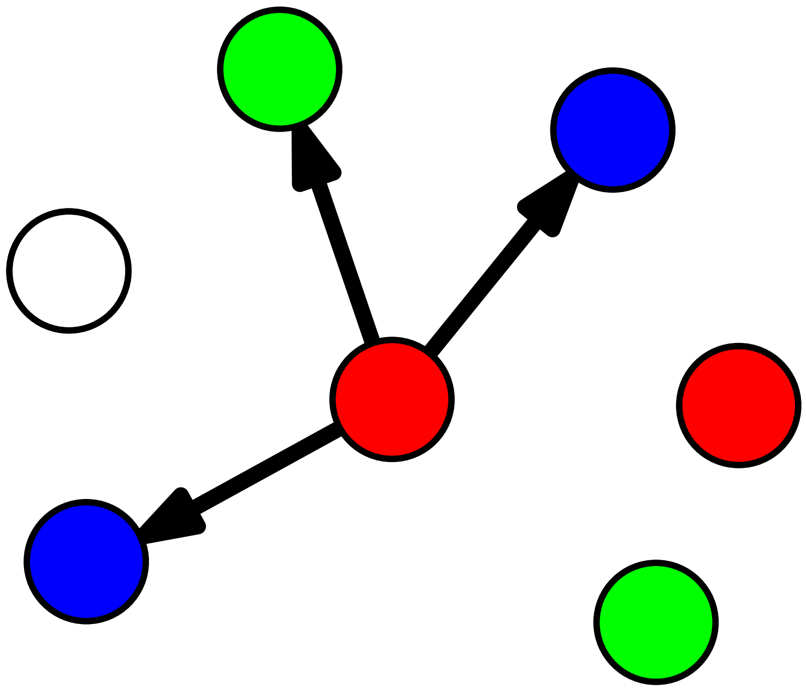
3-Median Dynamics

No almost validity!



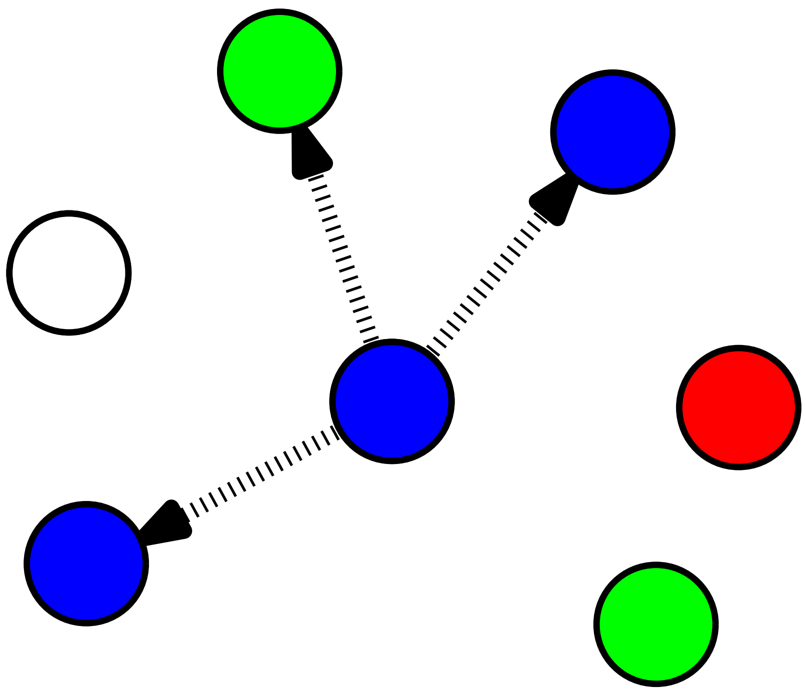
The adversary can manipulate the system.

The 3-Majority Dynamics



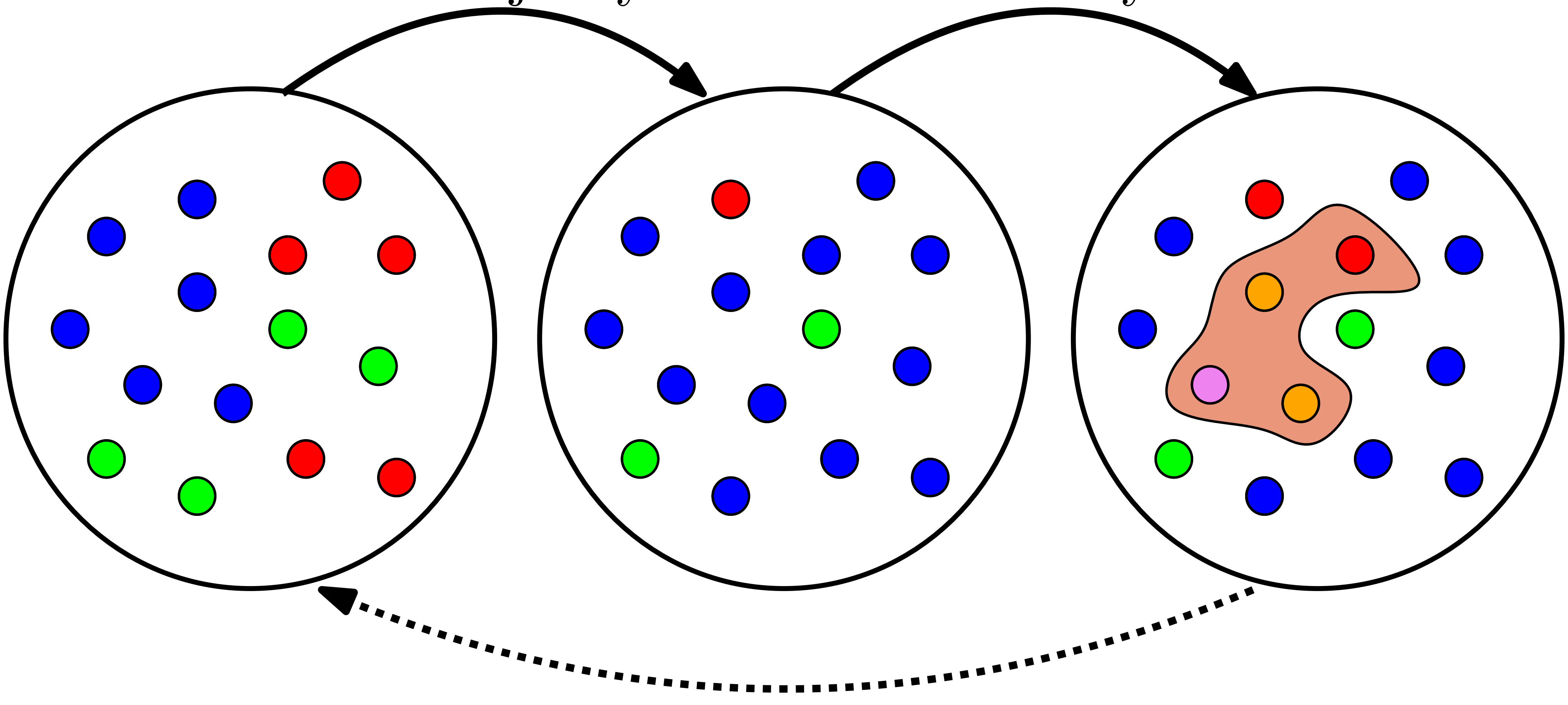
Each node observes the color of three other nodes chosen u.a.r....

The 3-Majority Dynamics



...and changes its color according to the majority of these three (breaking ties u.a.r.).

The Majority Process



Almost consensus? Almost validity? Almost stability?

3-Majority for Plurality Consensus

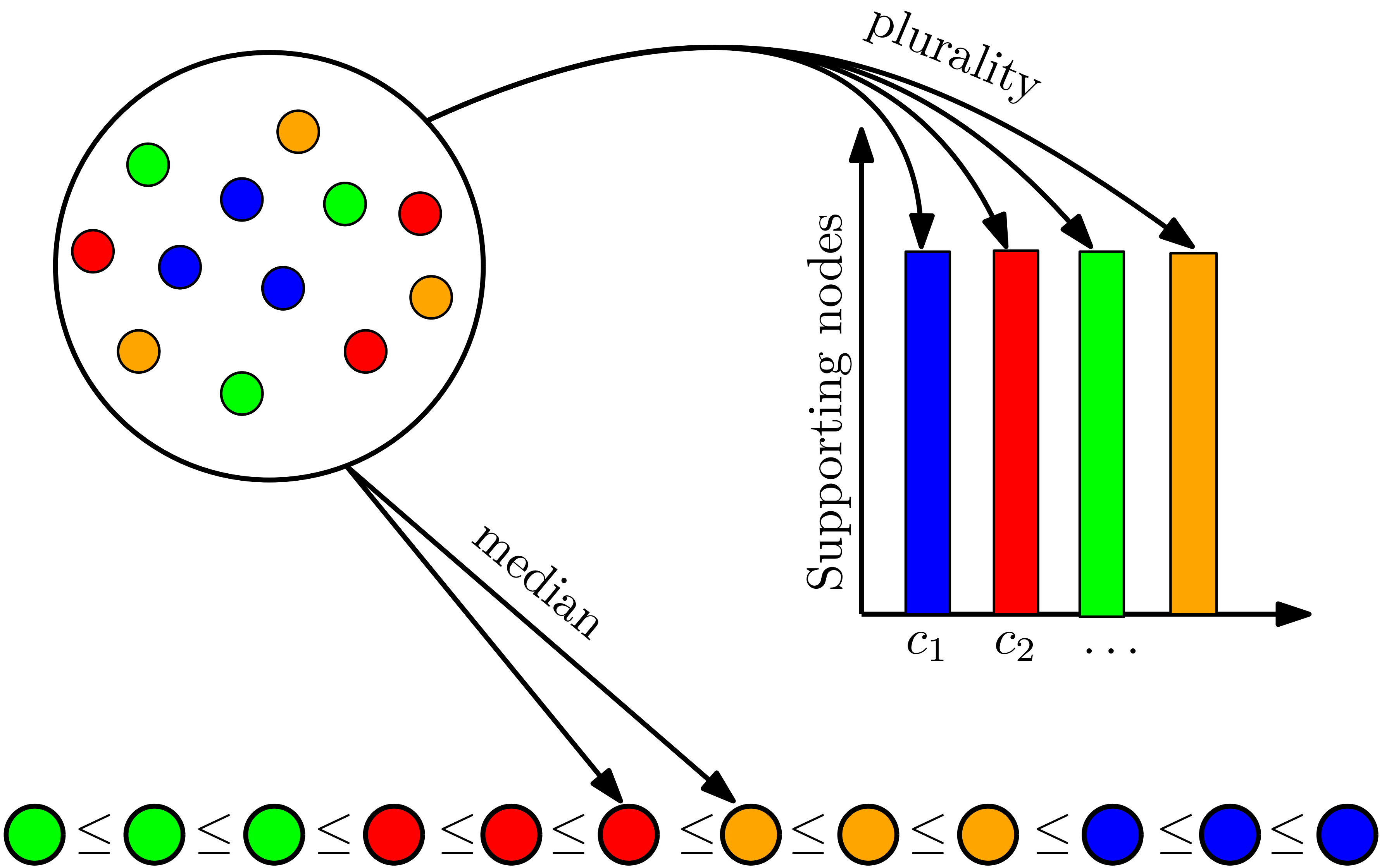
$c_i^{(t)} := |\{i\text{-colored nodes}\}|$ color 1 is the plurality

Initial bias s: For all $i \neq 1$, $c_1 - c_i \geq s$

Theorem (Becchetti, Clementi, Natale, Pasquale, Silvestri, Trevisan '14).

- From any configuration with $k < \sqrt[3]{n}$ colors, with bias $s = \Omega(\sqrt{kn \log n})$, the **3-majority** converges to the plurality color in $O(k \log n)$ rounds w.h.p., against a $O(\sqrt{n})$-bounded dynamic adversary.
- From configurations where every color is supported by almost n/k nodes, convergence takes $\Omega(k)$ rounds w.h.p.

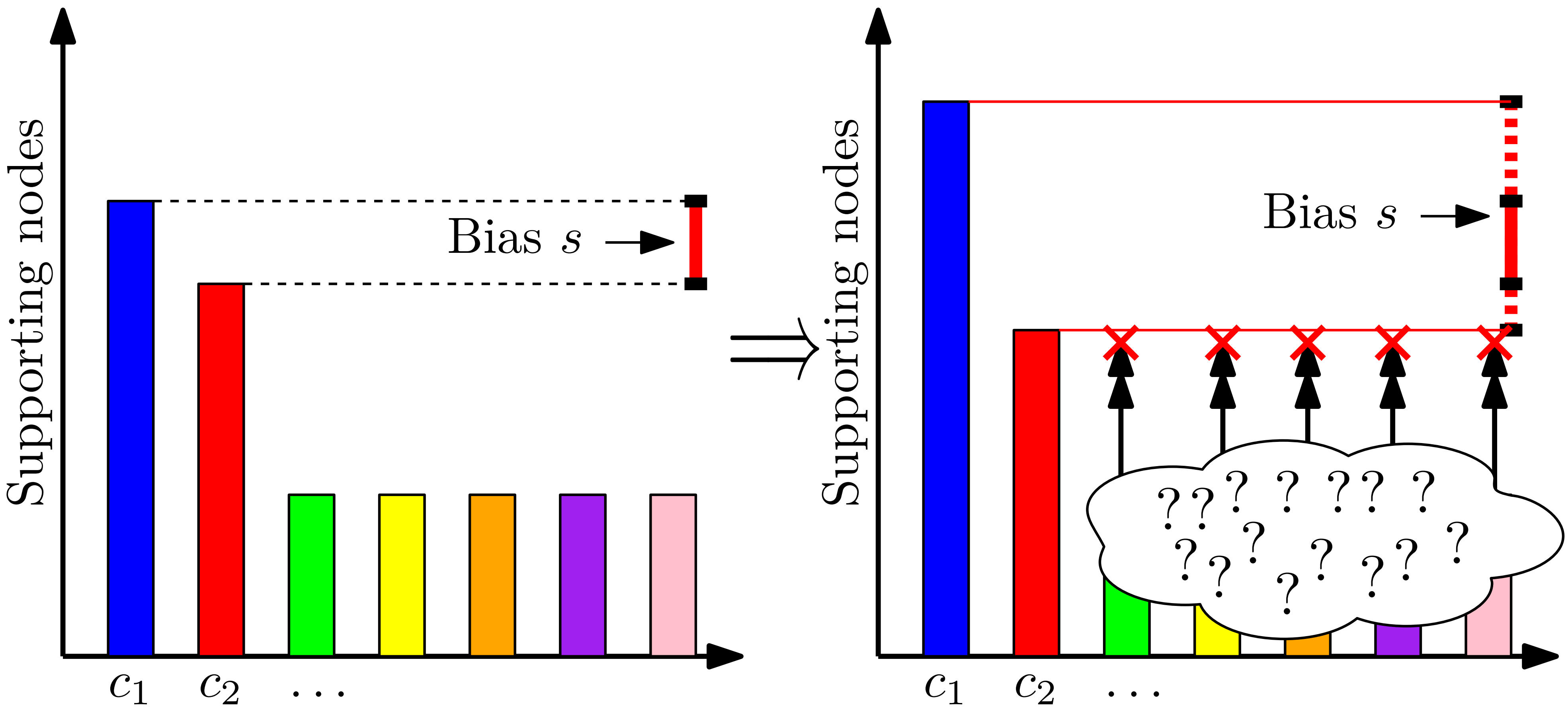
3-Majority vs 3-Median



3-Majority with Bias

$c_i^{(t)} := |\{i\text{-colored nodes}\}|$ color 1 is the plurality

Initial bias s**:** For all $i \neq 1$, $c_1 - c_i \geq s$



Our Contribution: 3-Majority without Bias

What if we start from any initial configuration, i.e. there may be no initial bias?

Theorem. Let $k \leq n^{\alpha}$, for a suitable constant $\alpha < 1$, and $F = \mathcal{O}(\sqrt{n}/(k^{\frac{5}{2}} \log n))$. The 3-majority dynamics is a stabilizing almost-consensus protocol against any F-dynamic adversary, with convergence time $\mathcal{O}((k^2\sqrt{\log n} + k \log n)(k + \log n))$, w.h.p.

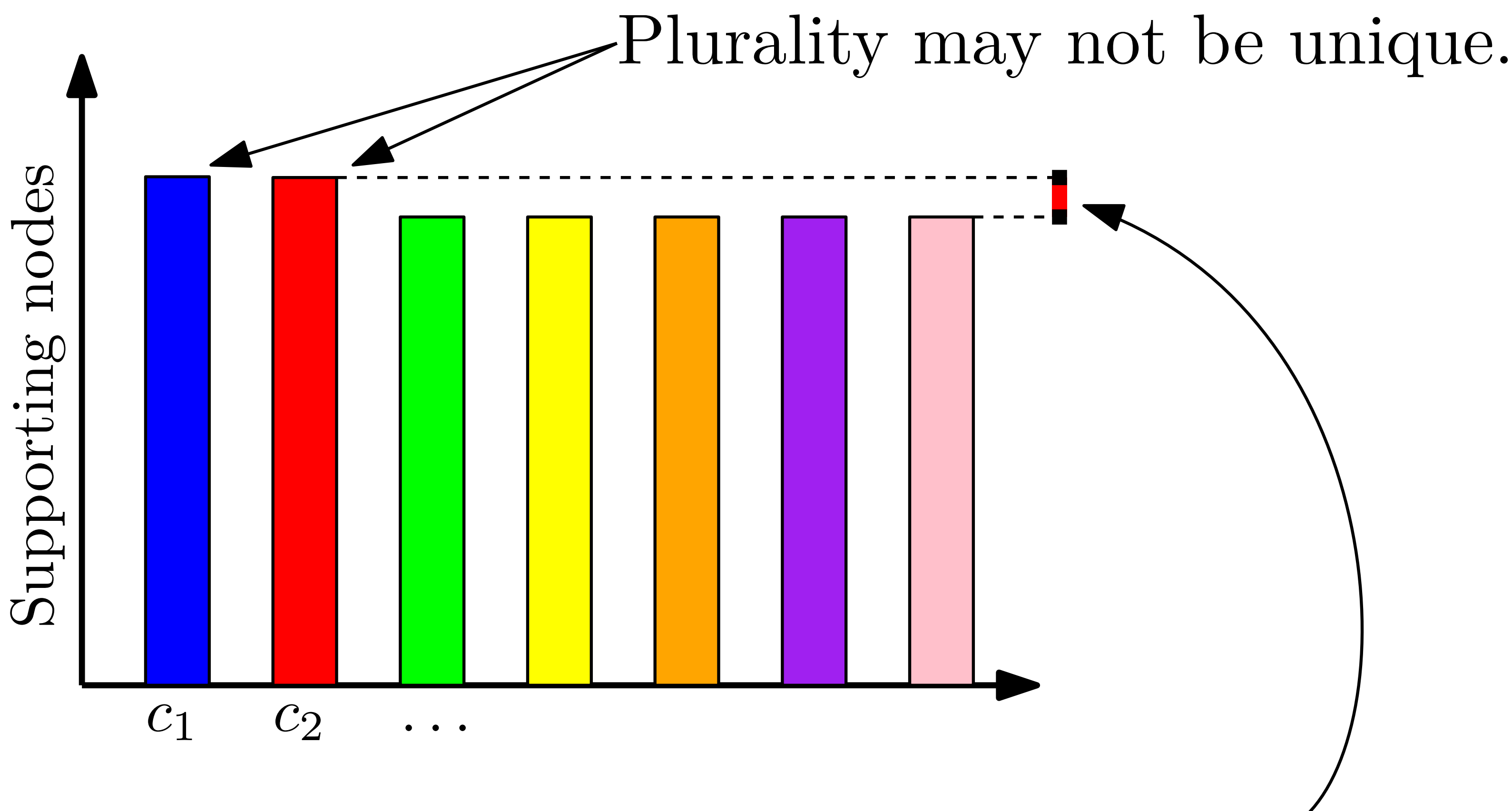
Our Contribution: 3-Majority without Bias

What if we start from any initial configuration, i.e. there may be no initial bias?

Theorem. Let $k \leq n^{\alpha}$, for a suitable constant $\alpha < 1$, and $F = \mathcal{O}(\sqrt{n}/(k^{\frac{5}{2}} \log n))$. The 3-majority dynamics is a stabilizing almost-consensus protocol against any F-dynamic adversary, with convergence time $\mathcal{O}((k^2\sqrt{\log n} + k \log n)(k + \log n))$, w.h.p.

- First solution of the almost-stabilizing consensus problem in the uniform gossip model.
- Closes open question on convergence of 3-majority for $|\Sigma| > 2$.

The Problem without Bias



Very small gap between the plurality colors and second colors: one of the second colors may become plurality.

Analysis of 3-Majority

$C_i^{(t)}$:= number of nodes supporting color i at round t.

$\mu_j(\mathbf{c}) = \mathbf{E}[C_j^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}]$

Lemma 1. For any color j it holds

$$\mu_j(\mathbf{c}) = c_j\left(1 + \frac{c_j}{n} - \frac{1}{n^2}\sum_{h\in[k]} c_h^2\right).$$

Lemma 2. Let 1 be a plurality color and j be a second-most-frequent color, then

$$\mu_1 - \mu_j \geqslant s(\mathbf{c})\left(1 + \frac{c_1}{n}\left(1 - \frac{c_1}{n}\right)\right).$$

Analysis of 3-Majority

$C_i^{(t)}$:= number of nodes supporting color i at round t.

$\mu_j(\mathbf{c}) = \mathbf{E}[C_j^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}]$

Lemma 1. For any color j it holds

$$\mu_j(\mathbf{c}) = c_j\left(1 + \frac{c_j}{n} - \frac{1}{n^2}\sum_{h\in[k]} c_h^2\right).$$

Lemma 2. Let 1 be a plurality color and j be a second-most-frequent color, then

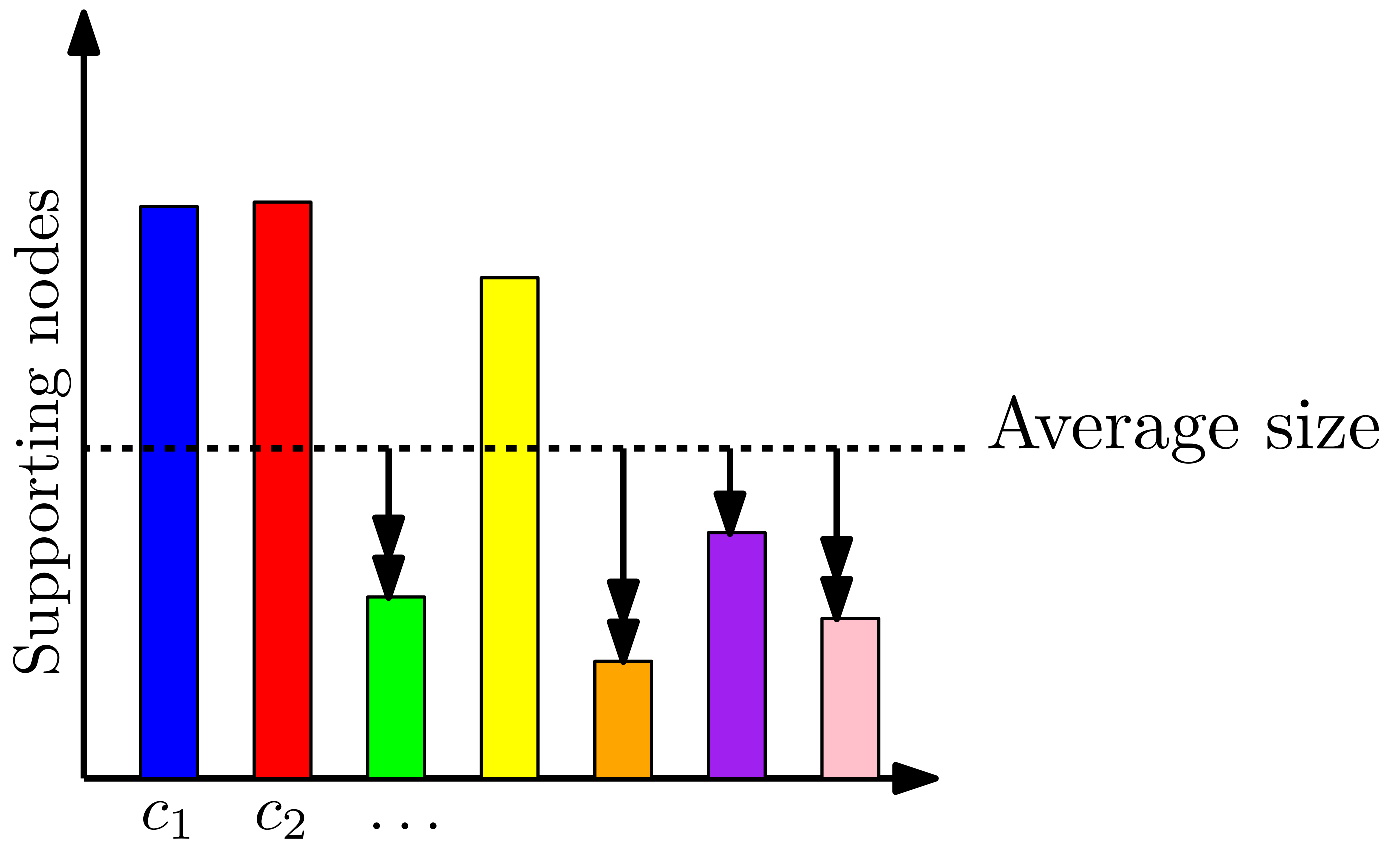
$$\mu_1 - \mu_j \geqslant s(\mathbf{c})\left(1 + \frac{c_1}{n}\left(1 - \frac{c_1}{n}\right)\right).$$

Indices are random variables: without bias, cannot concentrate on who is the plurality.

New Approach: Minorities Disappear

Lemma. Let $\mathbf{c}$ be the conf. at round t with j supported colors. For any color i it holds,

$$\mathbf{E}[C_i^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}] \leq c_i \left(1 + \frac{c_i}{n} - \frac{1}{j}\right).$$



A “dying phase”

Lemma. Let $\mathbf{c}$ be any conf. with $j \leq n^{1/3-\varepsilon}$ supported colors ($\forall \varepsilon > 0$ const), and such that an color i exists with $c_i \leq n/j - \sqrt{jn \log n}$. Within $t = \mathcal{O}(j \log n)$ rounds color i becomes $\mathcal{O}\left(j^2 \log n\right)$ w.h.p.

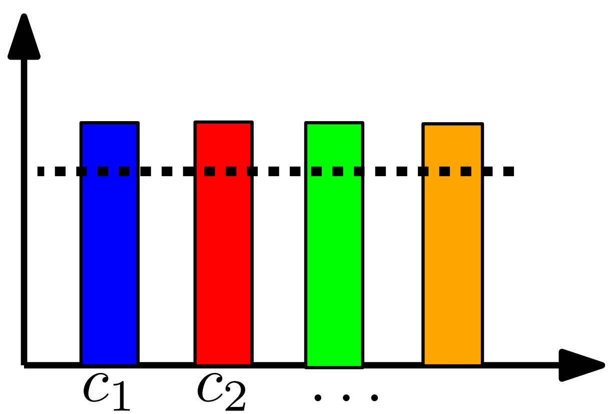
$$c_i \leq n/j - \sqrt{jn \log n} \xrightarrow[\text{w.h.p.}]{t = \mathcal{O}(j \log n)} c_i = \mathcal{O}(j^2 \log n)$$

A "dying phase"

Lemma. Let $\mathbf{c}$ be any conf. with $j \leq n^{1/3-\varepsilon}$ supported colors ($\forall \varepsilon > 0$ const), and such that an color i exists with $c_i \leq n/j - \sqrt{jn \log n}$. Within $t = \mathcal{O}(j \log n)$ rounds color i becomes $\mathcal{O}\left(j^2 \log n\right)$ w.h.p.

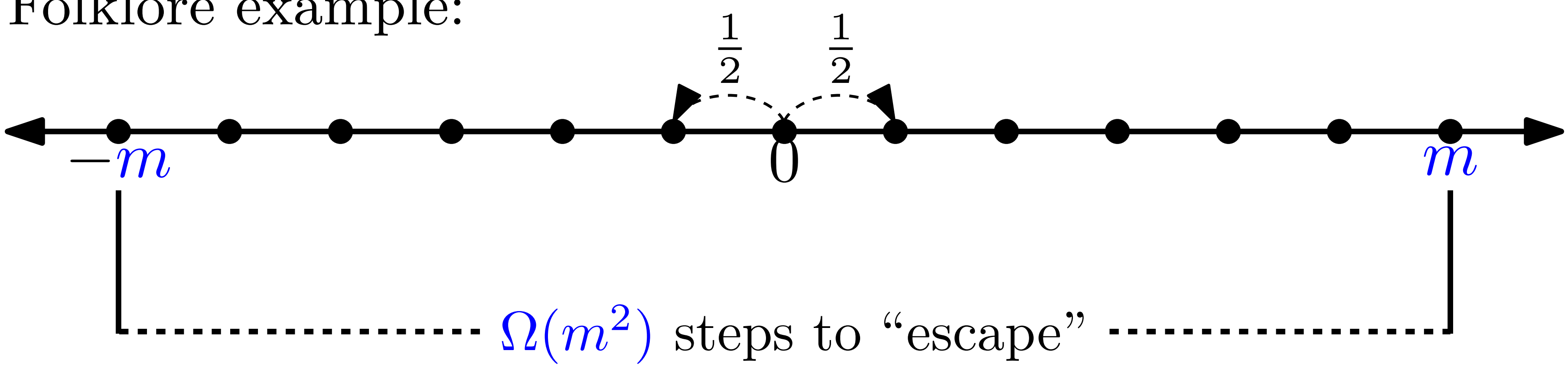
$$c_i \leq n/j - \sqrt{jn \log n} \xrightarrow[\text{w.h.p.}]{t = \mathcal{O}(j \log n)} c_i = \mathcal{O}(j^2 \log n)$$

How to reach such imbalance from any configuration?

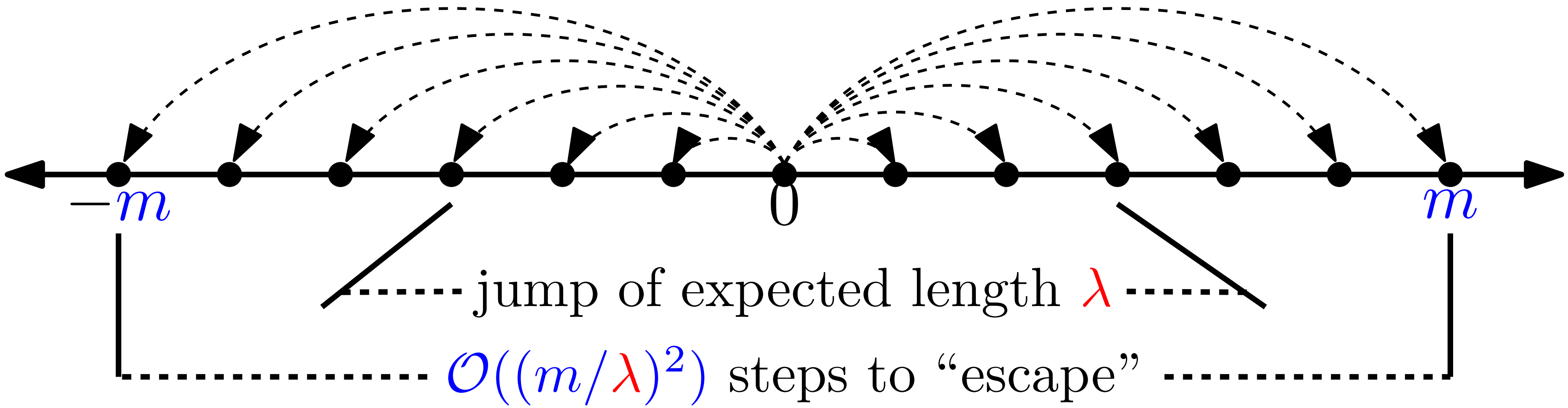


Simmetry Breaking

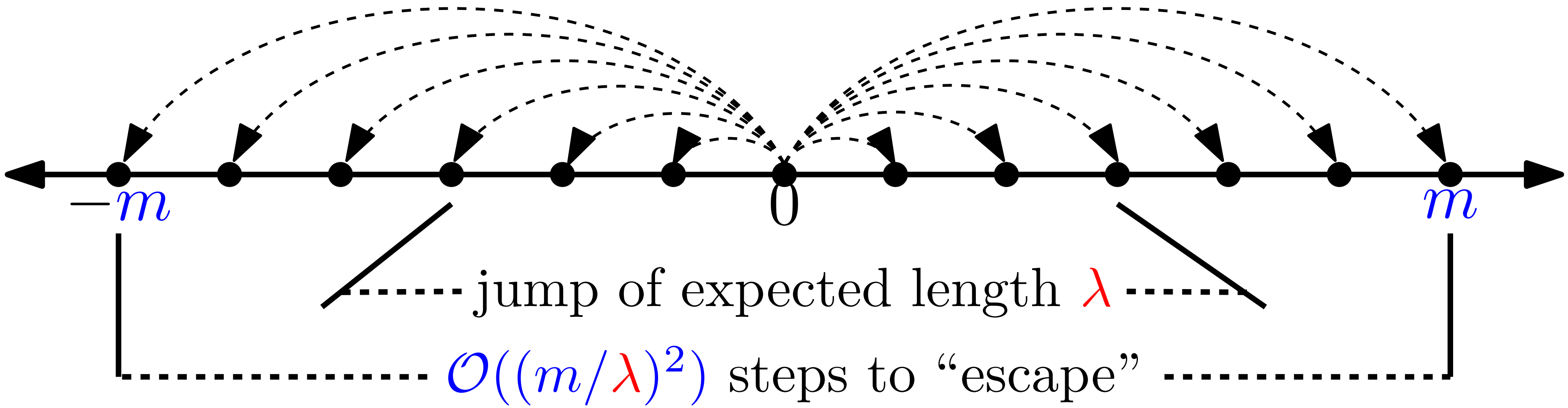
Folklore example:



Simmetry Breaking



Simmetry Breaking



Lemma 42.
$\{X_t\}_t$ a Markov chain with finite state space Ω,
$f : \Omega \to \mathbf{N}$, $Y_t = f(X_t)$,
$m \in [n]$ a “target value” and $\tau = \inf\{t \in \mathbb{N} : Y_t \geq m\}$.
If $\forall x \in \Omega$ with $f(x) \leq m - 1$, it holds

1. *Positive drift*: $\mathbf{E}[Y_{t+1} \mid X_t = x] \geqslant f(x) + \lambda$ $(\lambda > 0)$,
2. *Bounded jumps*: $\Pr\{Y_\tau \geq \alpha m\} \leq \alpha m/n$, $(\alpha > 1)$,

then

$$\mathbf{E}[\tau] \leq 2\alpha \frac{m}{\lambda}.$$

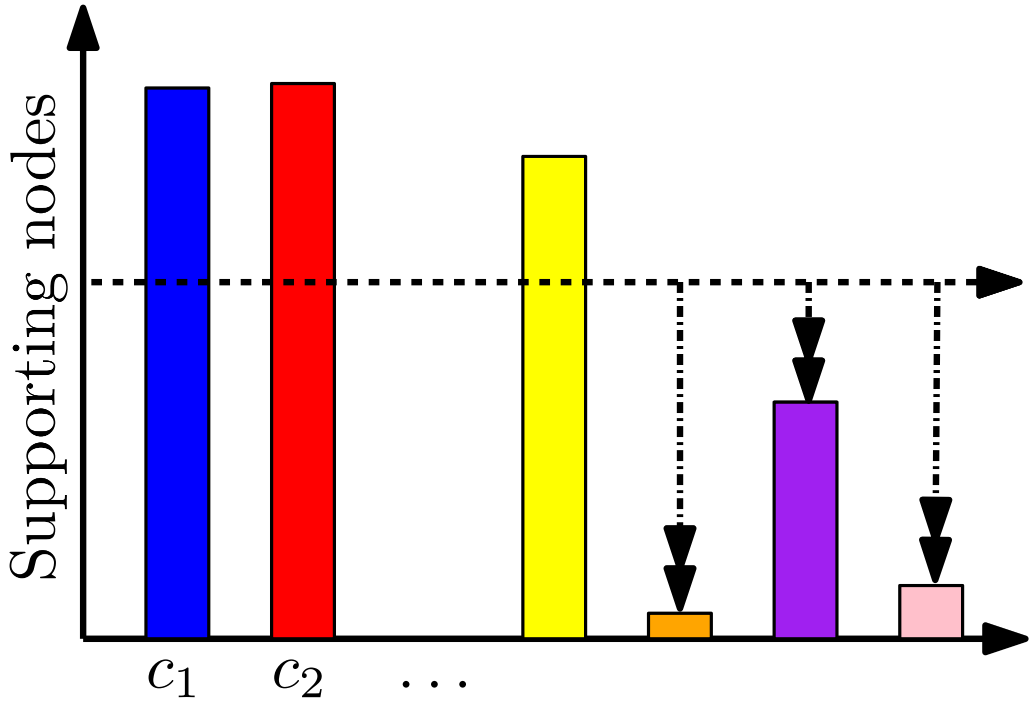
Simmetry Breaking

Lemma. Let $\mathbf{c}$ be any configuration with j supported colors. Within $t = \mathcal{O}\left(j^2\sqrt{\log n}\right)$ rounds it holds that

$$\Pr(\exists i \text{ such that } C_i^{(t)} \leq n/j - \sqrt{jn\log n}) \geq \frac{1}{2}$$

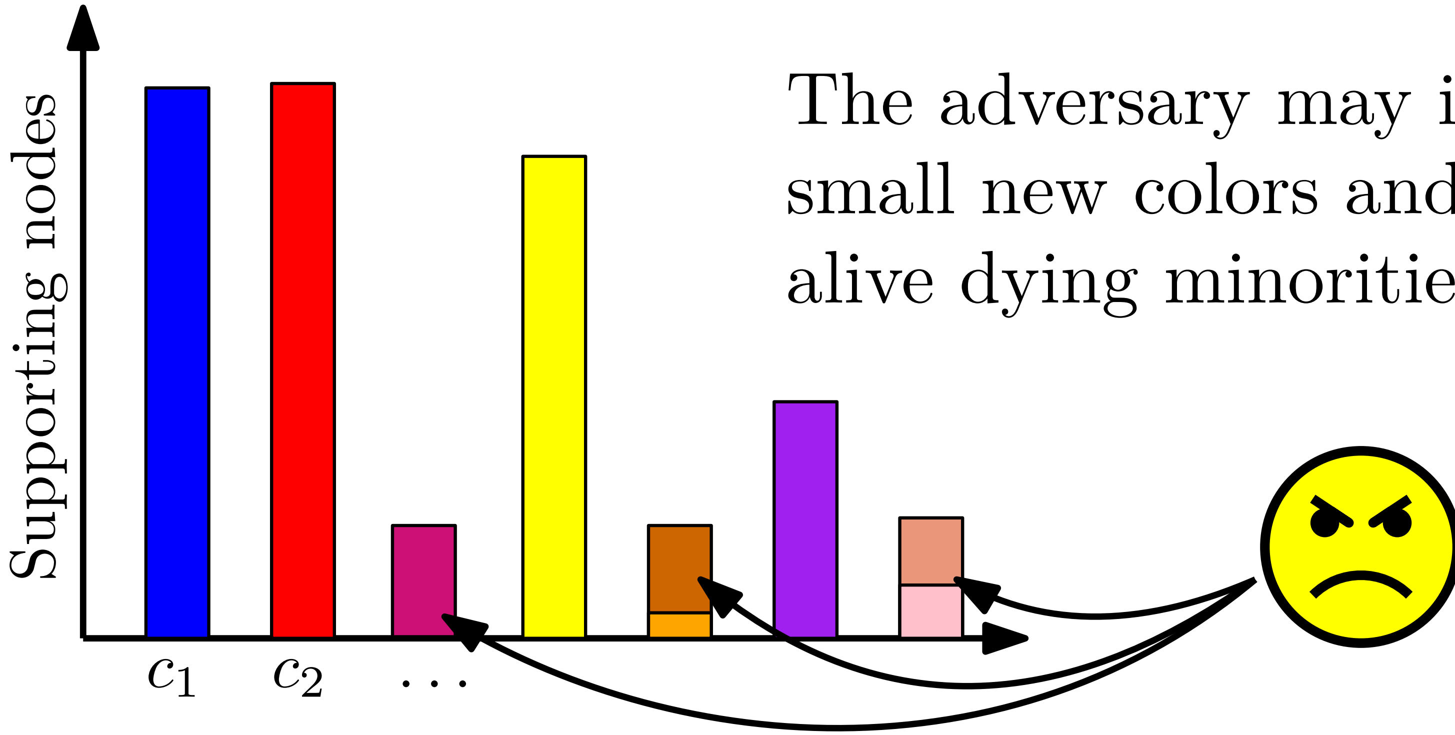
Proof. Let $\mathbf{m}(t)$ be the *index of minimum-size color* and apply Lemma 42 with $f(\mathbf{c}) = C_{\mathbf{m}(t)}$.

Handling the Adversary

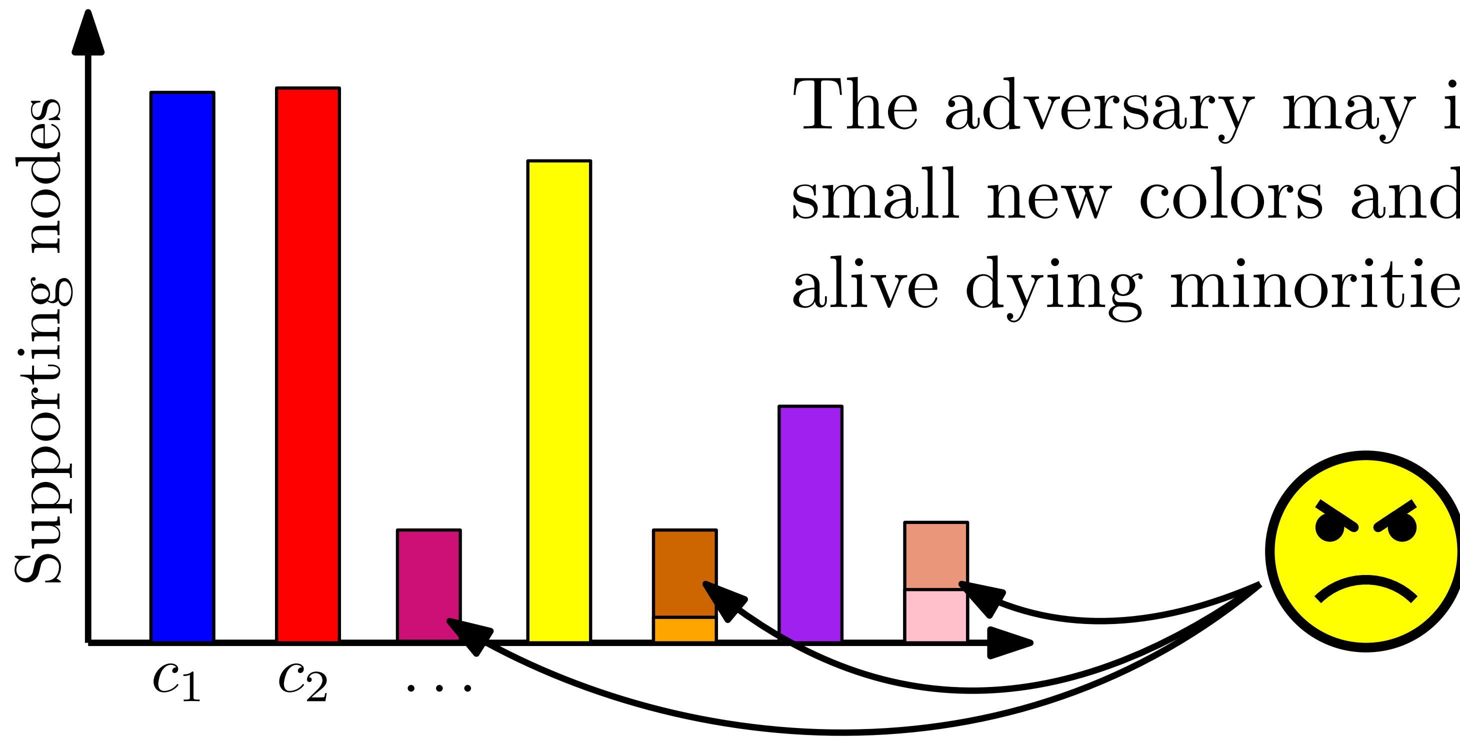


Handling the Adversary

The adversary may introduce small new colors and keep alive dying minorities.



Handling the Adversary



The adversary may introduce small new colors and keep alive dying minorities.

$$\mathbf{E}[C_i^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}] \leq c_i \left(1 + \frac{c_i}{n} - \frac{1}{j}\right)$$

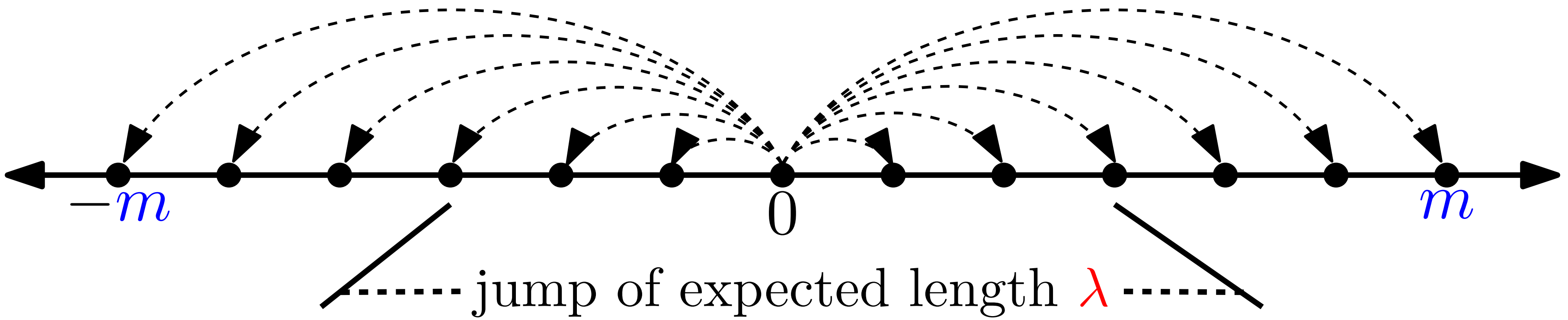
Supported colors

$$\mathbf{E}[\tilde{C}_i^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}] \leq c_i \left(1 + \frac{c_i}{n} - \frac{1}{j} + \sqrt{\frac{k}{n}}\right)$$

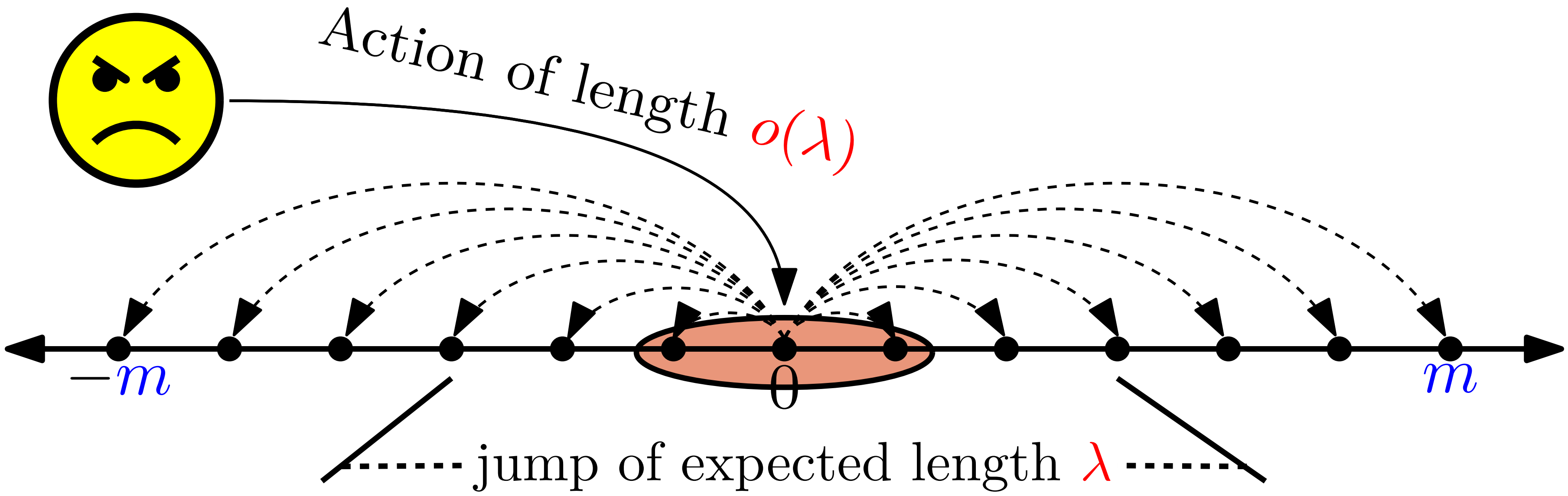
$F = \mathcal{O}\left(\frac{\sqrt{n}}{(k^{\frac{5}{2}} \log n)}\right)$

“Big” colors

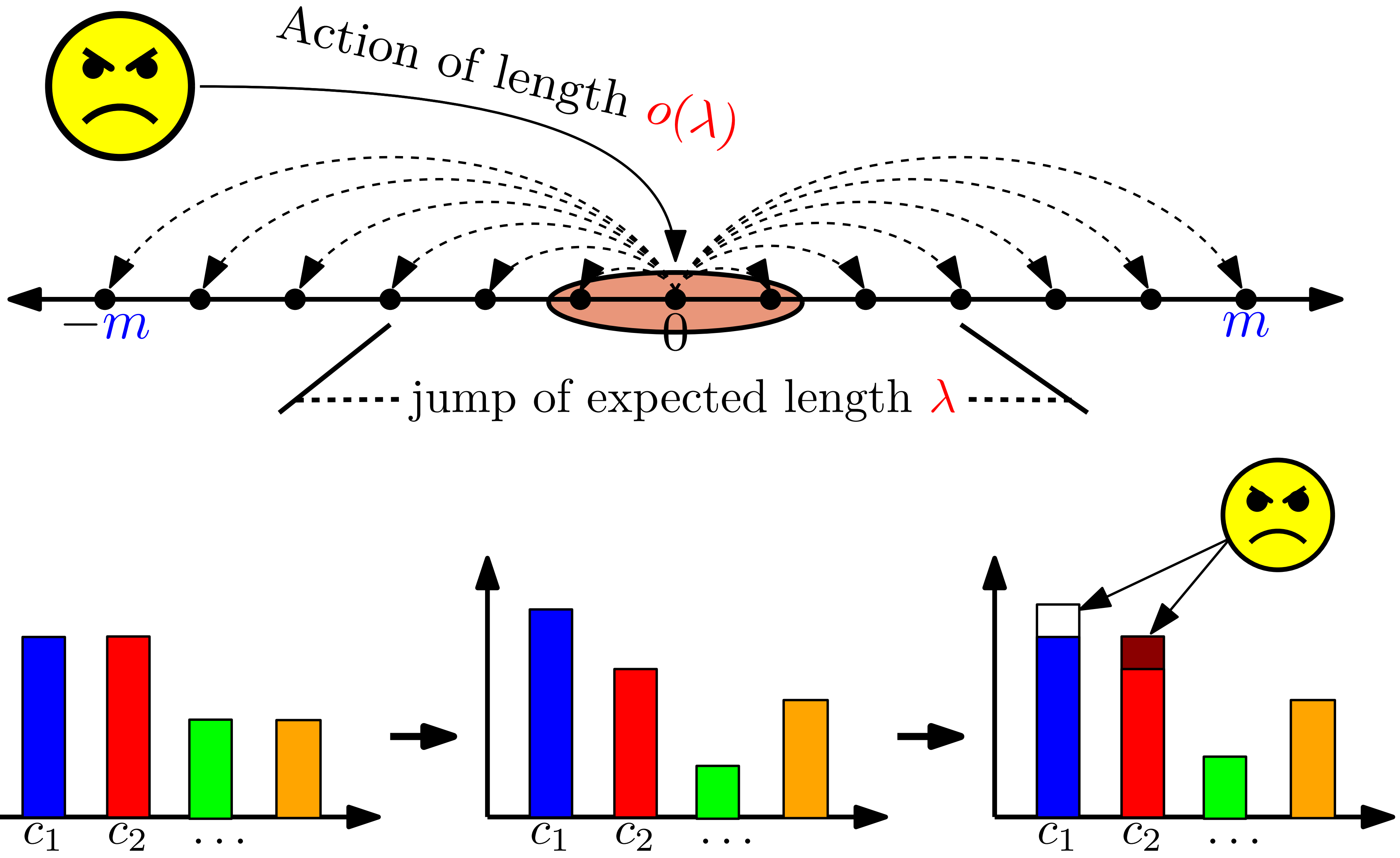
Handling the Adversary



Handling the Adversary



Handling the Adversary



Open Problems

- Convergence in time $\mathcal{O}(k \log n)$?

- Stabilizing consensus on random/expander graphs?

Thank you!