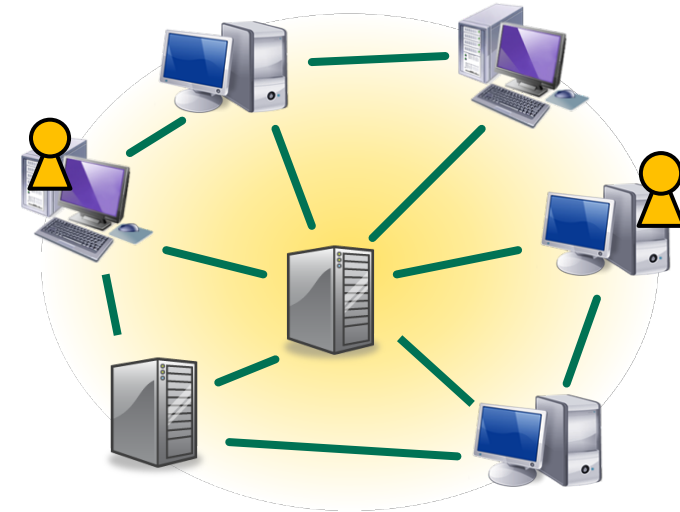


ビザンチンエージェントが混在する環境に おけるモバイルエージェントの集合問題

法政大学 首藤裕一
令和4年3月10日

モバイルエージェント

- **計算機間を自律的に移動**するソフトウェア
 - プログラムコードやメモリの内容とともに計算機間を移動
 - 移動先でプログラムの実行を継続
 - 以下、単に**エージェント**と呼ぶ
- 利用例
 - データの探索
 - 故障検知
 - etc...

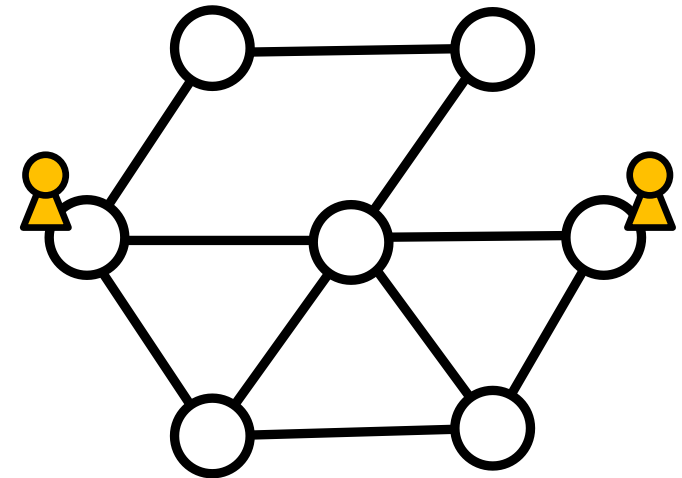
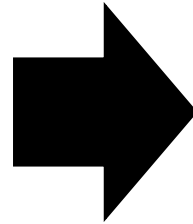
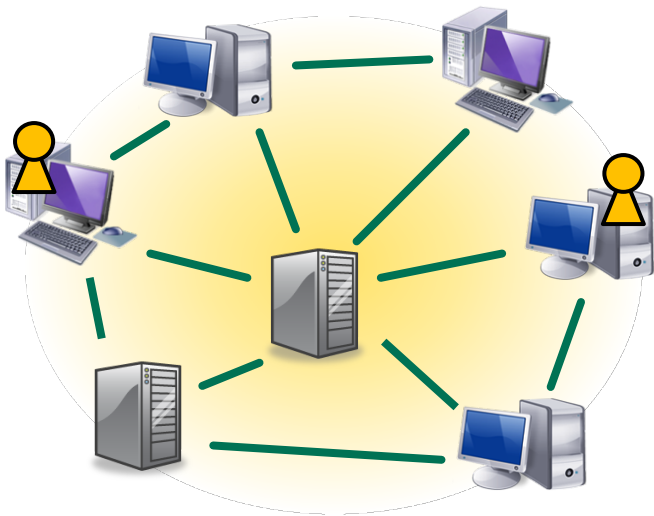


👤: モバイルエージェント

備考

頂点数を n 、辺数を m と表記

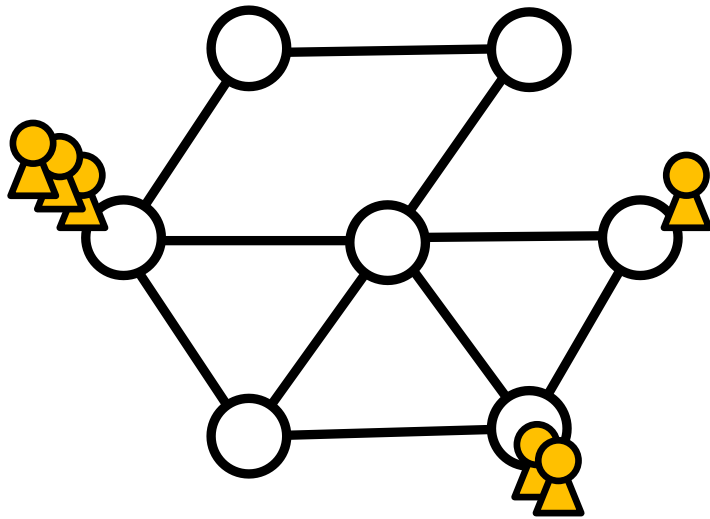
- 以降、ネットワークをグラフで表現します
 - 計算機 → 頂点
 - 通信リンク → 辺



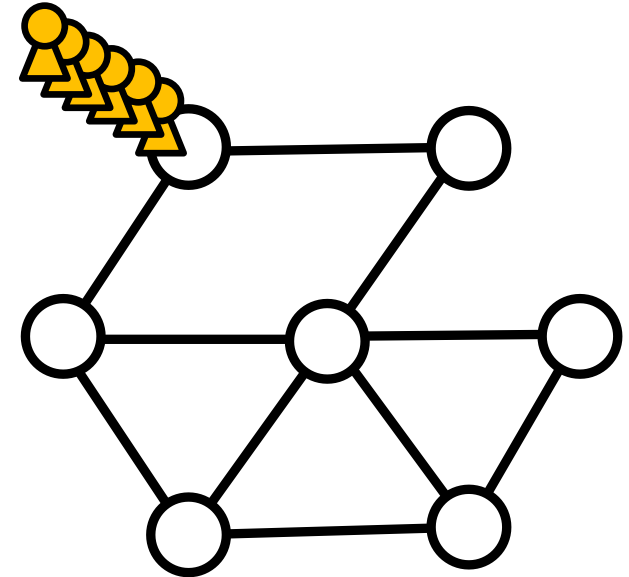
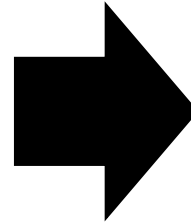
集合問題

エージェントが2体のときに限定した集合問題を
邂逅問題 (rendezvous) と呼ぶ

問題の仕様：すべてのエージェントがひとつの頂点に集まり、停止



初期状況

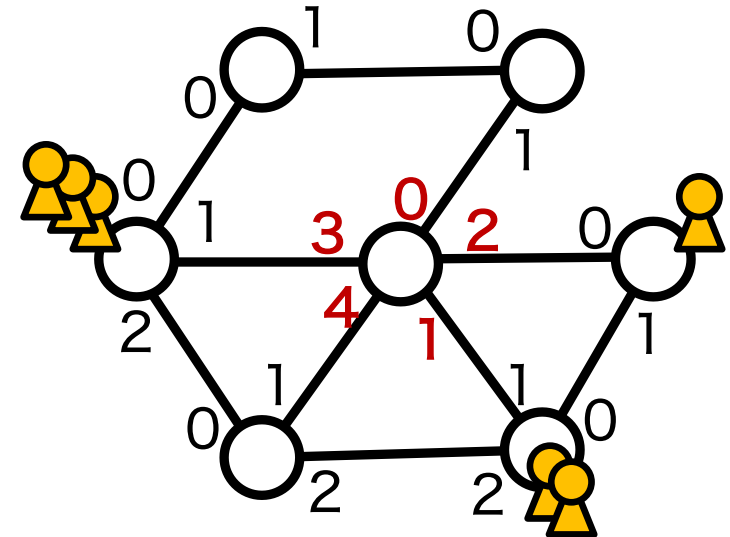


解状況

任意の初期配置から集合
できなければならない

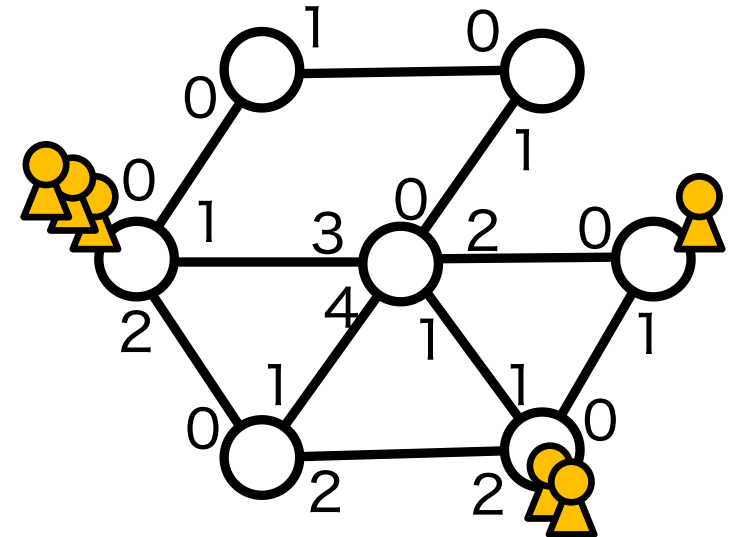
モデル (1/2)

- 頂点はIDを持たない (匿名グラフ)
- 各辺は両端の頂点で局所的に一意的な**ポート番号**を持つ
 - 頂点 v の接続辺のポート番号の集合は $\{1, 2, \dots, \delta_v\}$
 - ここで δ_v は v の次数
- エージェントは一意的なIDを持つ



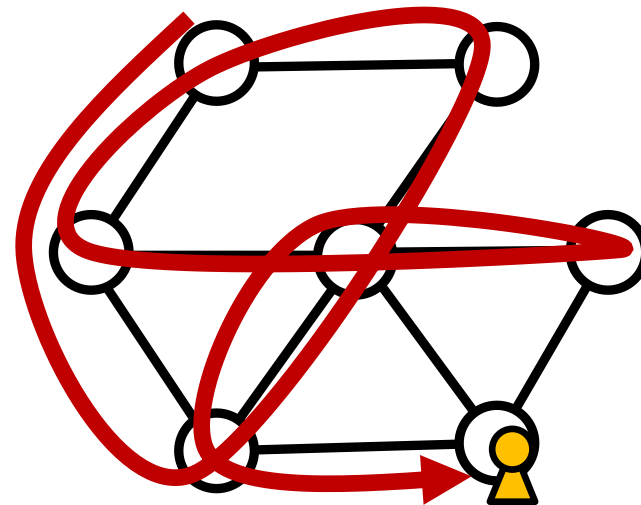
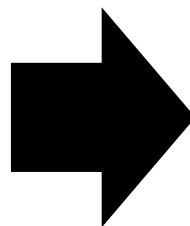
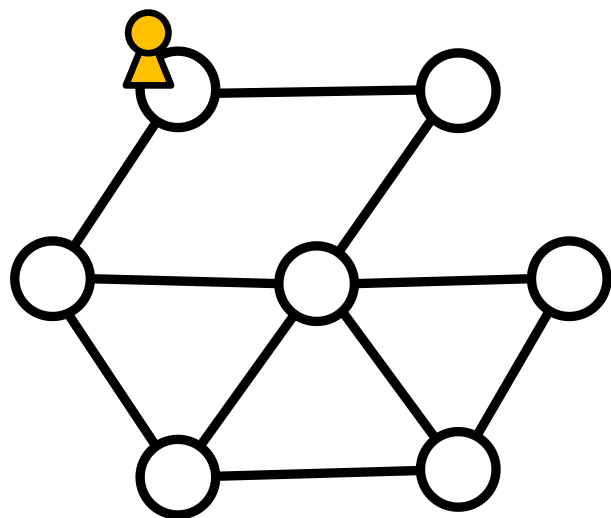
モデル (2/2)

- エージェントは同期して動作
 - 各時刻 $t = 0, 1, 2, \dots$ において全エージェントはアルゴリズムに従い以下を繰り返す
 - 同一頂点にいるエージェントと通信、
 - 自身の状態を更新 (i.e., メモリの内容を更新し)、
 - 隣接頂点に移動
- } ここに要する通信・計算時間は無視
- 時刻0で全エージェントは同じ状態 s_0
 - 初期状態 s_0 はアルゴリズムが定める



探索問題（集合問題と密接に関連！）

問題の仕様：1体のエージェントがいずれ全頂点を訪問し、停止

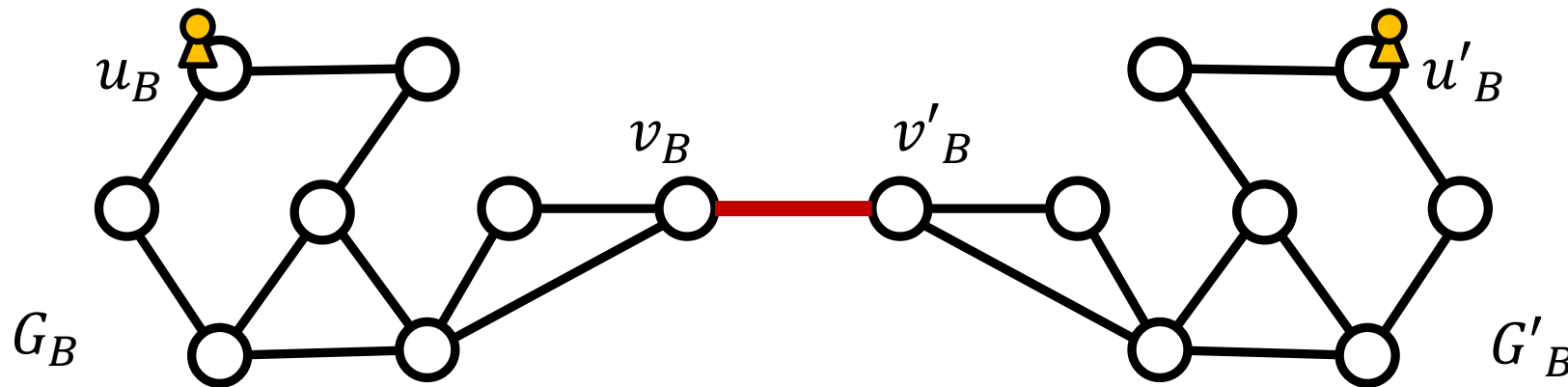


集合問題と探索問題の関連

集合問題を解くためには探索問題を解く必要がある

証明

- 探索問題が解けないと仮定する
- すなわち、いかなるアルゴリズム A に対しても、グラフ $G_A = (V_A, E_A)$ と頂点 $u_A, v_A \in V_A$ が存在し、 G_A 上で u_A から A を開始すると v_A を訪問しない
- すると、任意のアルゴリズム B について、 G_B とそのコピー G'_B を以下のように連結した初期状況からは、アルゴリズム B は集合を達成できない

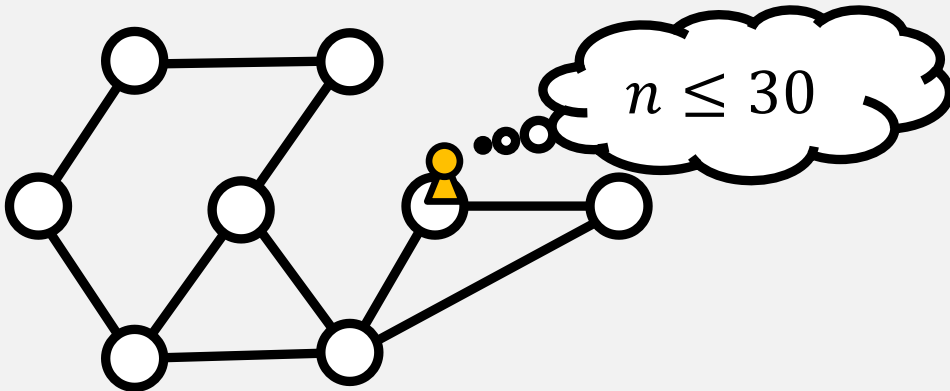


どのエージェントも
赤い辺を移動しない。
∴ 集合しない！

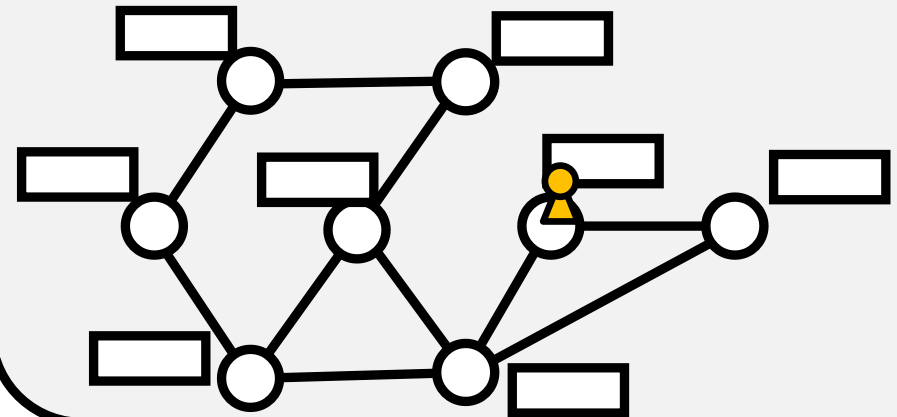
追加の仮定

- 前述のモデルそのままでは探索問題は解けない！
 - どれだけ移動しても全頂点を訪問したか確信が持てない
- したがって、集合問題も解けない！
 - エージェント数が既知の場合はこの限りではない
- なんらかの仮定を置く必要がある

仮定1：頂点数 n の上界 $N \geq n$ が既知

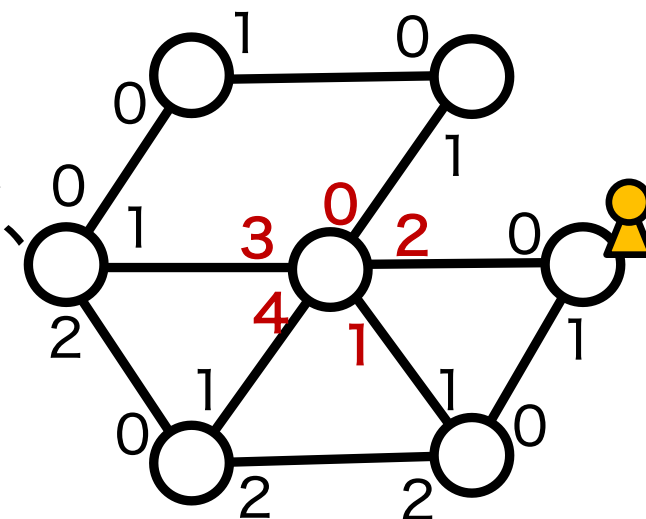


仮定2：白板の存在（後述）



頂点数 n の上界 $N \geq n$ が既知の場合の探索

- Alelinasら[1] (FOCS 1979) によるUXSで探索可能
 - UXS : 頂点数 N 以下のすべての連結グラフを探索可能なポート番号の列
 - UXSの長さは $\Theta(N^5 \log N)$
 - すなわち、UXSによる探索は $\Theta(N^5 \log N)$ 時間で十分
- 厳密にはAlelinasら[1]は正則グラフを仮定しているが、実は頂点数 N 以下の任意のグラフで探索可能
 - 少なくとも2007年にはTa-ShmaとZwick [2] (SODA 2007)が指摘

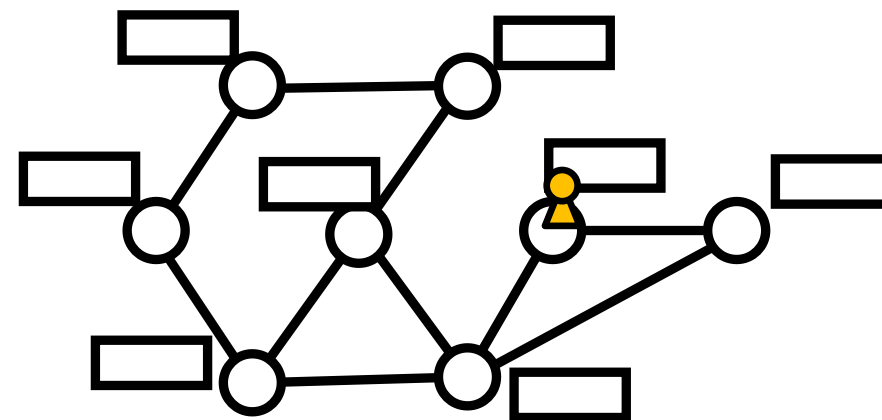


[1] Aleliunas, Romas and Karp, Richard M and Lipton, Richard J and Lovasz, Laszlo and Rackoff, Charles. "Random walks, universal traversal sequences, and the complexity of maze problems." 20th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, 1979.

[2] Ta-Shma, Amnon, and Uri Zwick. "Deterministic rendezvous, treasure hunts and strongly universal exploration sequences." *Symposium on Discrete Algorithms: Proceedings of the eighteenth annual ACM-SIAM symposium on Discrete algorithms*. Vol. 7. No. 09. 2007.

白板モデル

- エージェントが読み書き可能な頂点上のメモリ



- 白板があるとエージェントは各頂点にIDを与えることができる
- 深さ優先探索を行うことで $O(m)$ 時間で簡単に探索を達成可能
- 探索後、最小IDの頂点に移動することで**集合問題も簡単に解ける**

Ta-ShmaとZwickの邂逅アルゴリズム (SODA 2007)

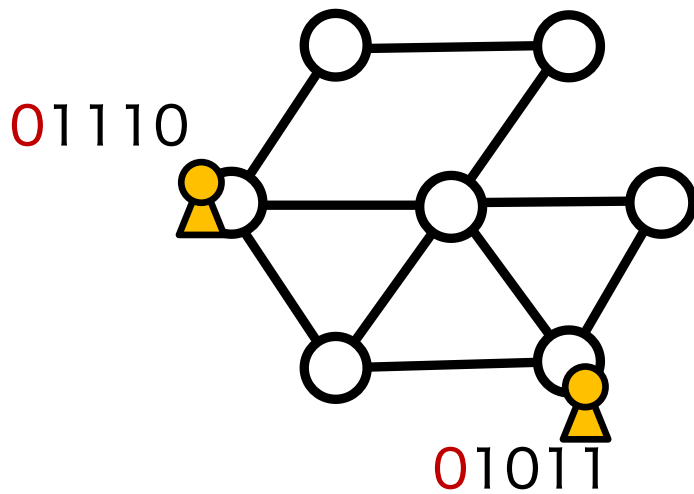
以降、**TZ法**と呼ぶ

邂逅問題 (再掲) :
エージェント数 $k=2$ のときの集合問題

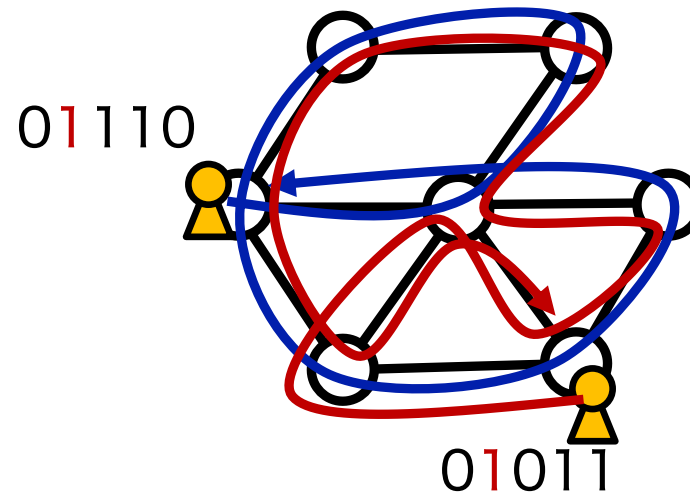
- 頂点数 n の上界 $N = O(n)$ を用いて $O(X(n)\lambda)$ 時間で邂逅問題を解く
 - $X(n)$: 探索に要する時間。ここでは $X(n) = O(n^5 \log n)$
 - λ : エージェントのID長
 - 厳密にはエージェントごとにID長は異なることを考慮して詳細な解析が行われることが多いのだが、本講演では簡単のためID長が等しいものとする
- 基本アイデア
 - 時刻 $i \cdot X(n) \sim$ 時刻 $(i + 1) \cdot X(n) - 1$ を第 i フェーズと呼ぶ
 - IDの2進表現が $b_0 b_1 \dots b_{\lambda-1}$ のエージェントは第 i フェーズにおいて以下を実行
 - $b_i = 1$ のとき : 探索アルゴリズムを実行
 - $b_i = 0$ のとき : 待機

2体のエージェントが出会うと終了

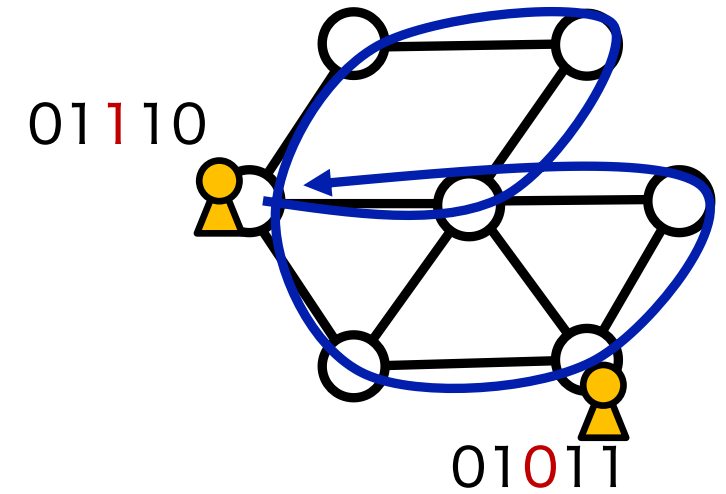
TZ法の実行例



1フェーズ目：
どちらも待機



2フェーズ目：
両方がグラフを探索。
すれ違うと出会わない



3フェーズ目：
一方が待機し、
もう一方が探索。
確実に会おう。

TZ法の一般化による集合

- 微修正により、一般のエージェント数 $k \geq 2$ に対してもTZ法を使える
 - 時刻 $i \cdot X(n) \sim$ 時刻 $(i + 1) \cdot X(n) - 1$ を第 i フェーズと呼ぶ
 - 各フェーズの開始時に同一頂点に存在するエージェント群を**集団**と呼ぶ
 - 集団内のエージェントの最小IDをその集団のIDとする
 - IDの2進表現が $b_0 b_1 \dots b_{\lambda-1}$ の集団は第 i フェーズにおいて以下を実行
 - $b_i = 1$ のとき：探索アルゴリズムを実行。待機中のエージェントを回収
 - $b_i = 0$ のとき：待機
- エージェント数 k の値に依らず $O(X(n)\lambda)$ 時間で集合達成
 - 第 i フェーズ開始時にどの集団もIDの末尾 $\lambda - i$ 桁が互いに異なることから自明

ここまでのまとめ

- (モバイル) エージェント：グラフ上を移動するソフトウェア
- 集合問題：任意の初期配置から全エージェントを一頂点に集めて停止
- 探索問題：1体のエージェントが全頂点を訪問して停止
- 探索問題が解けることは集合問題が解けることの必要条件
- 通常モデルに何らかの仮定を置かないと探索問題すら解けない
 - 頂点数 n の上界 $N \geq n$ が既知（通常 $N = O(n)$ を仮定）
 - 白板の存在を仮定
- 既知の上界 $N = O(n)$ があると $X(n) = O(n^5 \log n)$ でグラフの探索は可能
- **TZ法により、集合問題は $O(X(n)\lambda) = O(n^5 \lambda \log n)$ で解ける**
 - λ はエージェントのID長

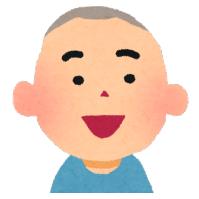
いよいよ ビザンチンエージェントの 登場です

本講演の題目：

ビザンチンエージェントが混在する環境における
モバイルエージェントの集合問題

ビザンチンエージェント（悪性エージェント）

- アルゴリズムから逸脱して任意の敵対的な行動を取るエージェント
 - 例1：アルゴリズムの動作とは異なる移動を行う
 - 例2：他のエージェントに偽の情報を流す

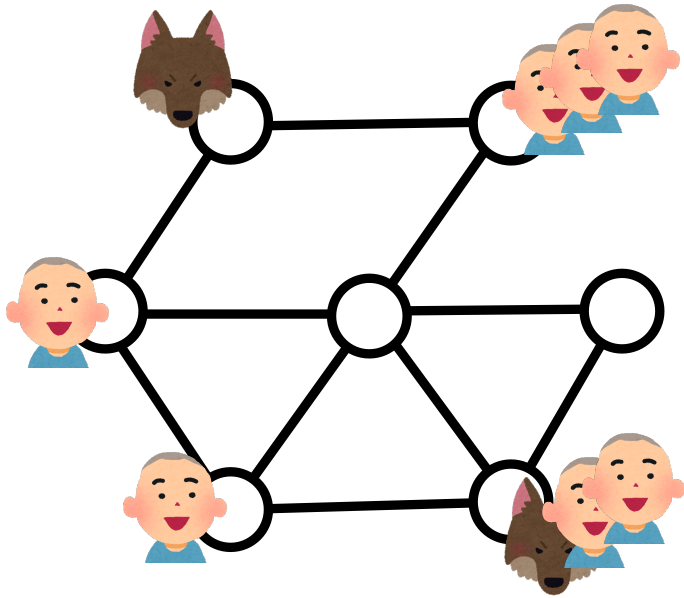


悪性エージェント 正常エージェント

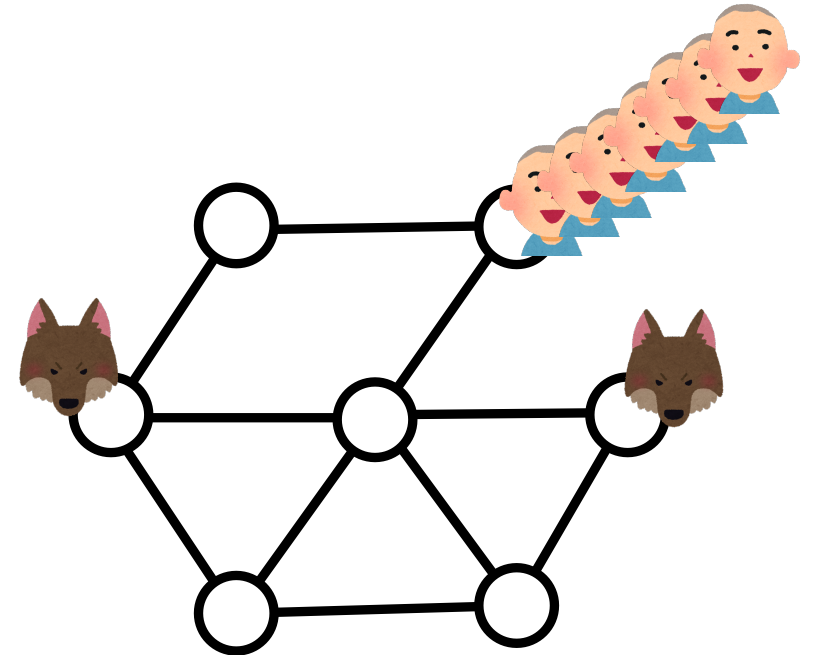
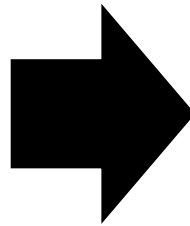
- 人狼ゲームにおける人狼のような存在
- 悪性エージェントは**あらゆる情報と無限の計算能力**を持つ
 - 離れている悪性エージェントどうしも連携可能
 - グラフの形状やポート番号を把握
 - 全エージェントの位置や状態（i.e., メモリの中身）をいつでも参照可能

ビザンチンあり集合問題

問題の仕様：すべての**正常エージェント**がひとつの頂点に集まり、停止



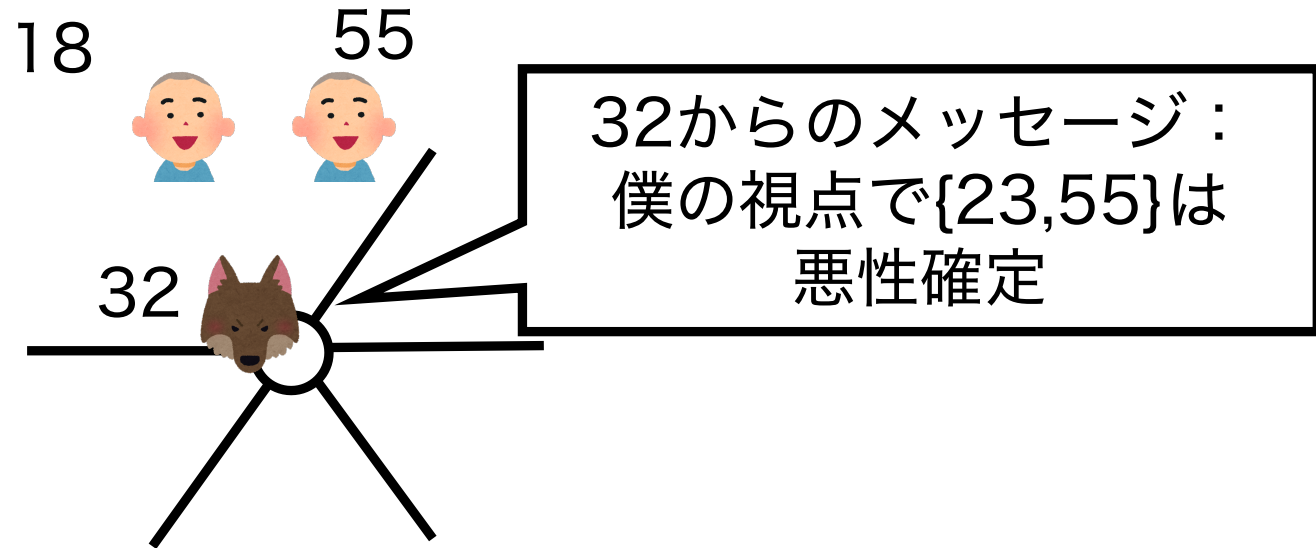
初期状況



解状況

悪性エージェントの制約

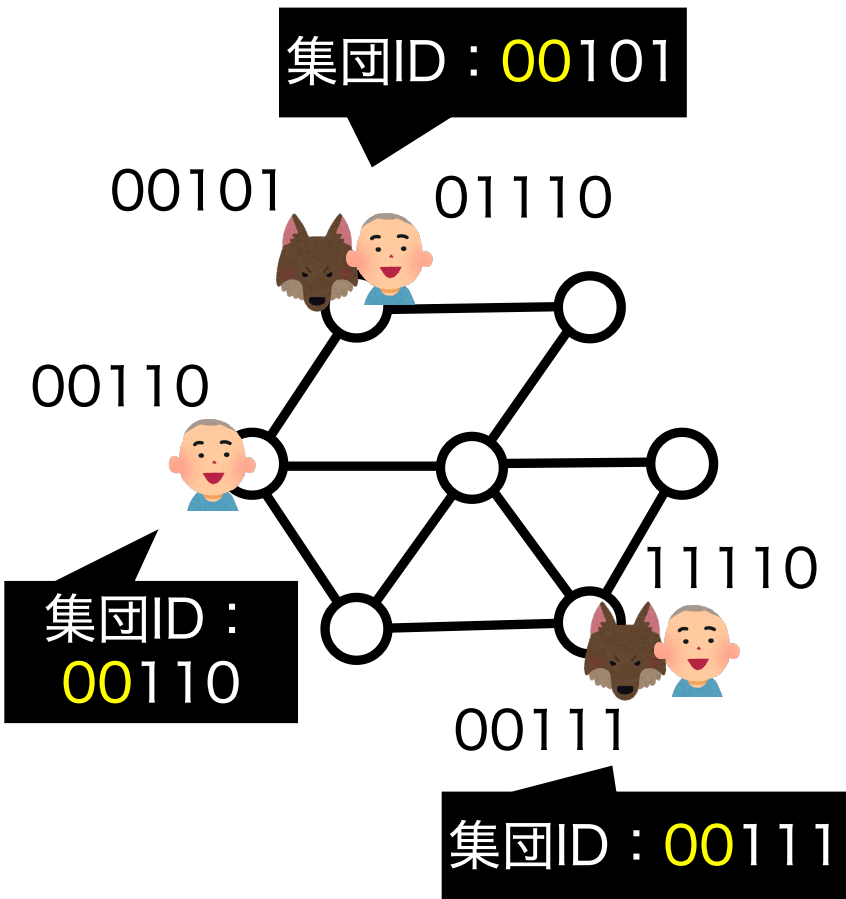
- このままでは問題が解けないので以下の2つの制約を課す



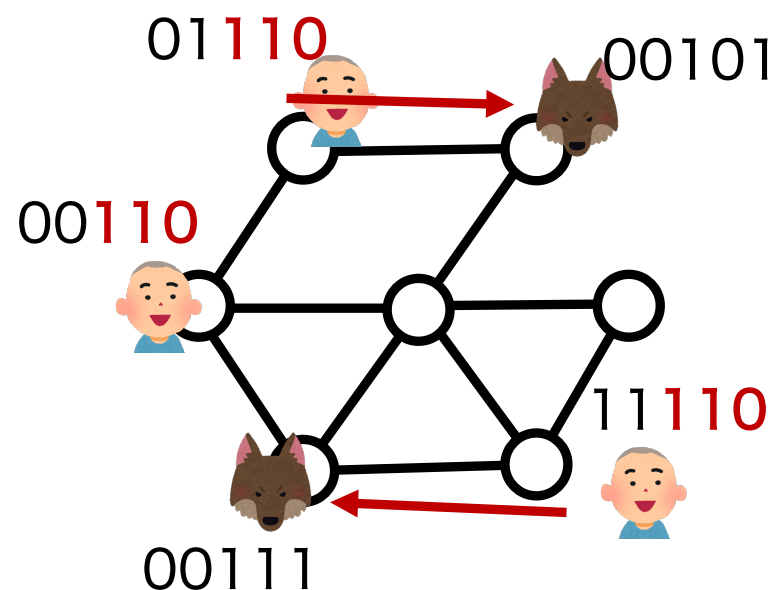
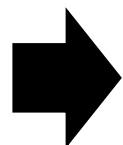
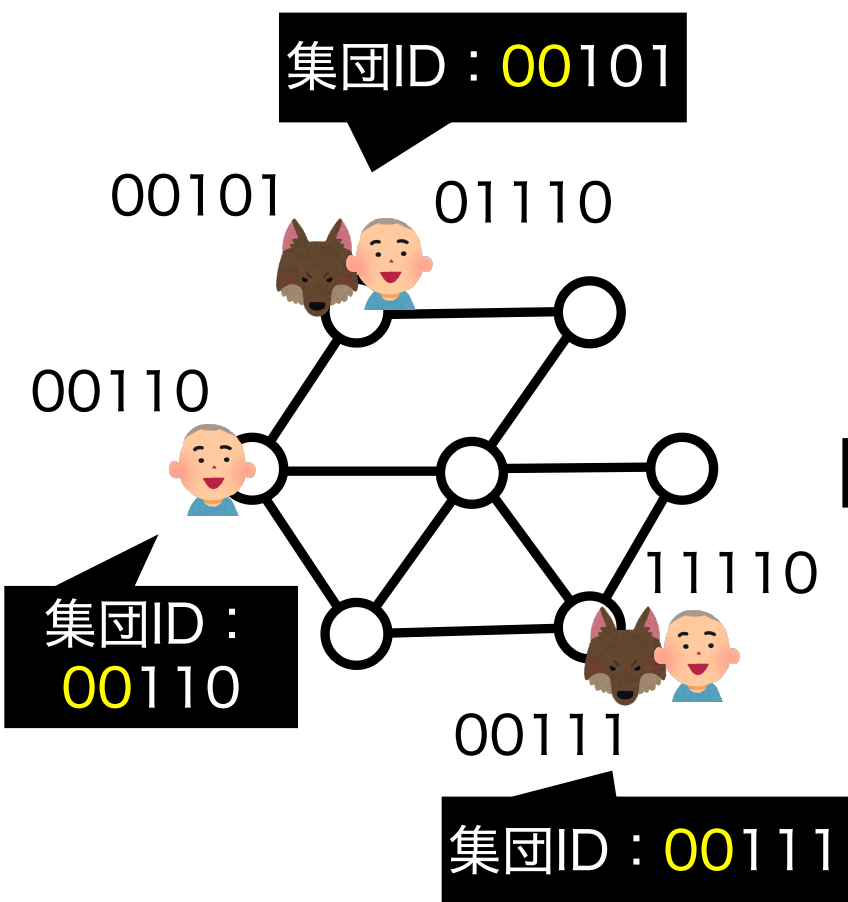
制約1：なりすまし不可
通信相手に自分のIDがバレる

制約2：「叫び」通信
同一頂点の全エージェントに
同じメッセージしか送れない

TZ法そのままでは歯が立たない

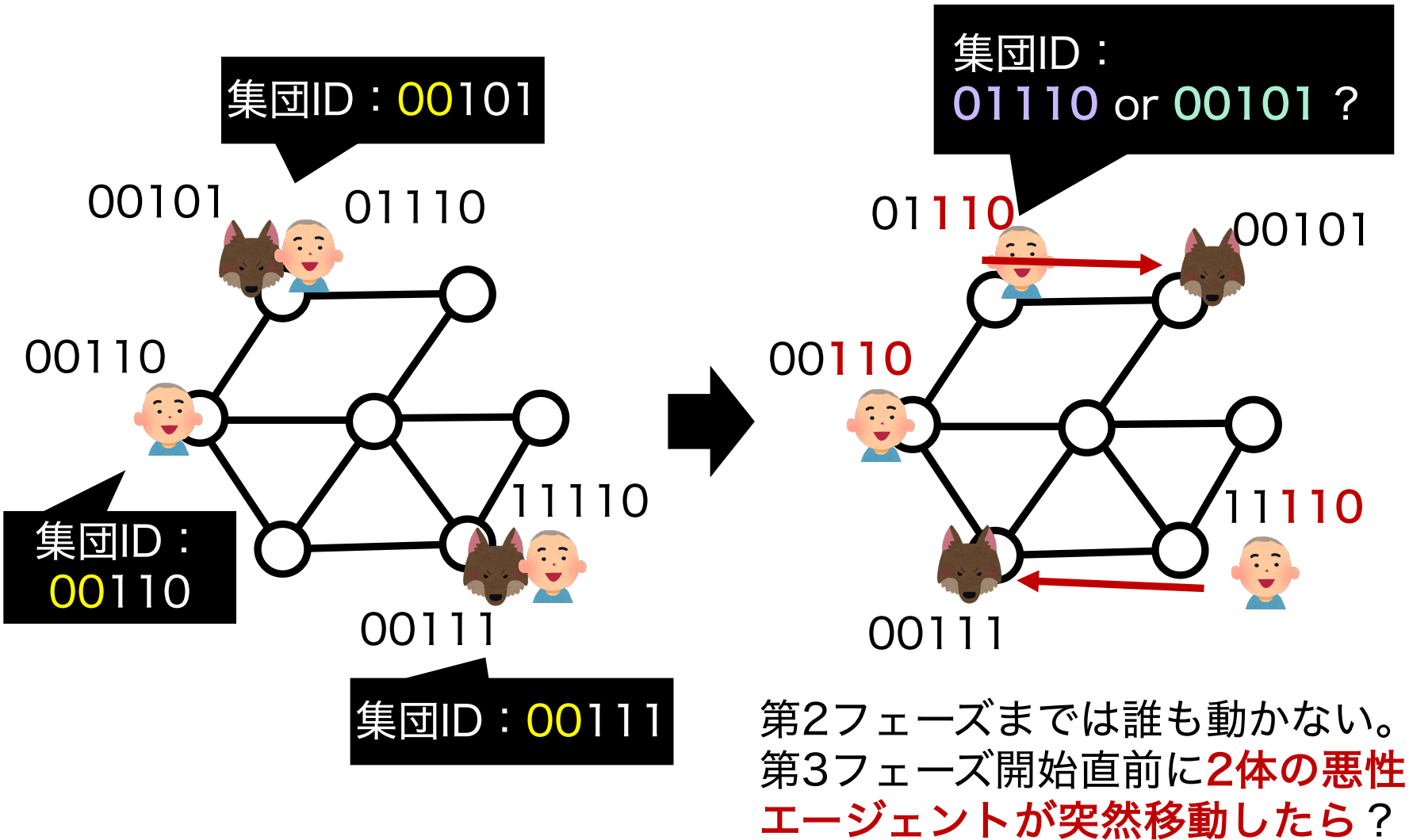


TZ法そのままでは歯が立たない

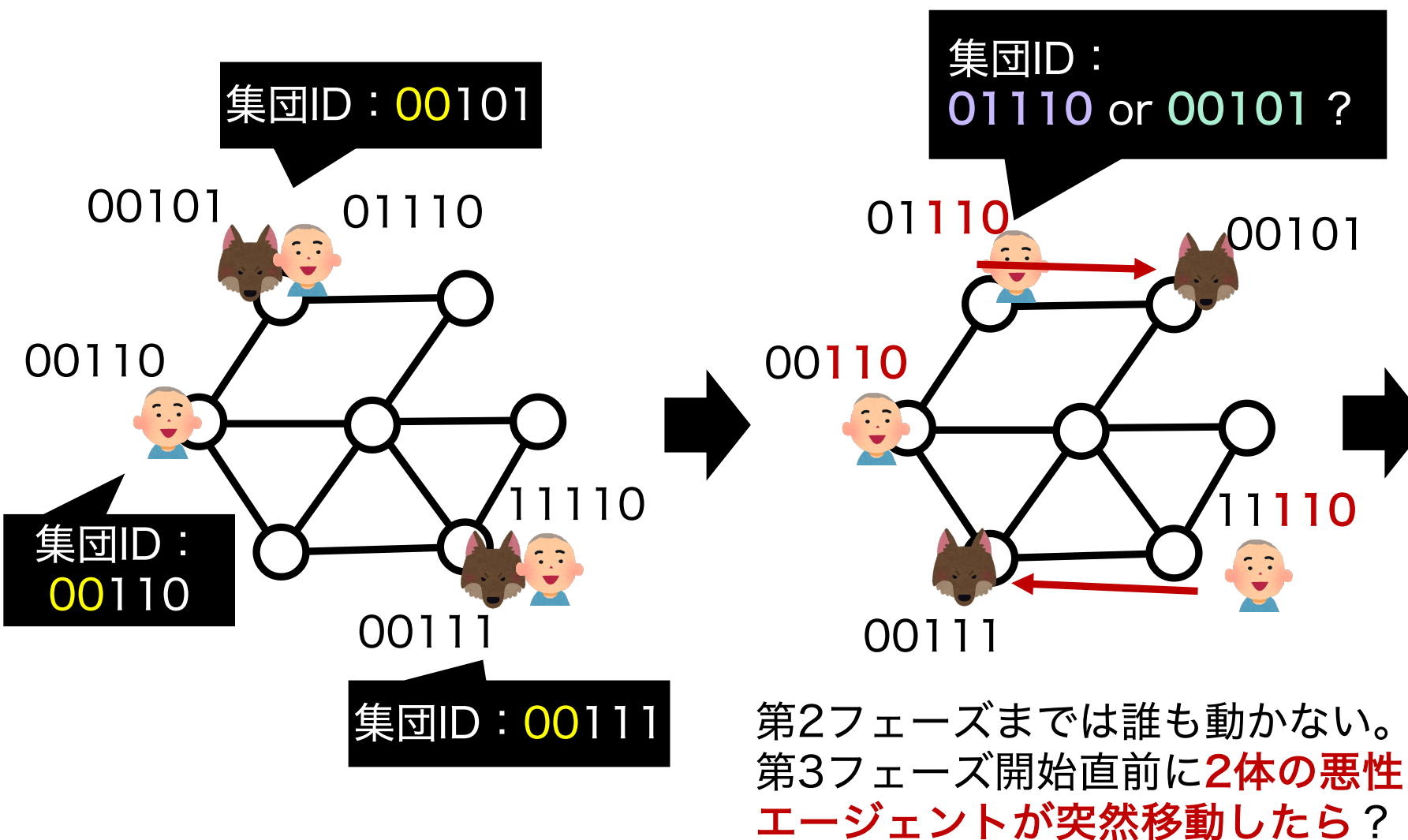


第2フェーズまでは誰も動かない。
第3フェーズ開始直前に**2体の悪性エージェント**が突然移動したら？

TZ法そのままでは歯が立たない



TZ法そのままでは歯が立たない



集団IDをフェーズ開始時の
最小IDとすると…
**3集団ともに末尾3桁が
110**なので集合が保証され
ない！

前フェーズの集団IDを固持
すると…
**集団内に集団IDを持つ
エージェントが存在しな
くなり**、待機エージェント
を回収できなくなる

ビザンチン集合アルゴリズム

	初期知識	悪性エージェント数の制約	白板	署名	時間計算量	成功率
Dieudonnéら[3]	N	なし	なし	なし	$O(k^2 f^2 \lambda \cdot X(n))$	1
鈴木・首藤	N	なし	なし	なし	$O(\mathbf{k} f \lambda \cdot X(n))$	1
Hiroseら[4]	N	$f = O(\sqrt{k})$	なし	なし	$O((f + \lambda) \cdot X(n))$	1
Hiroseら[5]	N, F	$F \leq (k - 1)/3$	なし	なし	$O(F \lambda \cdot X(n))$	1
Hiroseら[5]	N	$f \leq (k - 1)/9$	なし	なし	$O(f \lambda \cdot X(n))$	1
Tsuchidaら[6]	F	なし	あり	あり	$O(Fm)$	1
小杉・首藤	K	なし	あり	なし	$O(m + \alpha n K)$	$1 - 1/2^\alpha$

N : 頂点数 n の上界 ($n = O(N)$ を仮定) 、 f : 悪性エージェント数、
 F : 悪性エージェント数 f の上界、 K : エージェント数 k の上界、
 α : $\log K$ 以上の任意の整数

ビザンチン集合アルゴリズム

	初期 知識	悪性エー ジェント数の制約	白板	署名	時間計算量	成功率
Dieudonnéら[3]	N	なし	なし	なし	$O(k^2 f^2 \lambda \cdot X(n))$	1
鈴木・首藤	N	なし	なし	なし	$O(kf\lambda \cdot X(n))$	1
Hiroseら[4]	N	$f = O(\sqrt{k})$	なし	なし	$O((f + \lambda) \cdot X(n))$	1
Hiroseら[5]	N, F	$F \leq (k - 1)/3$	なし	なし	$O(F\lambda \cdot X(n))$	1
Hiroseら[5]	N	$f \leq (k - 1)/9$	なし	なし	$O(f\lambda \cdot X(n))$	1
Tsuchidaら[6]	F	なし	あり	あり	$O(Fm)$	1
小杉・首藤	K	なし	あり	なし	$O(m + \alpha n K)$	$1 - 1/2^\alpha$

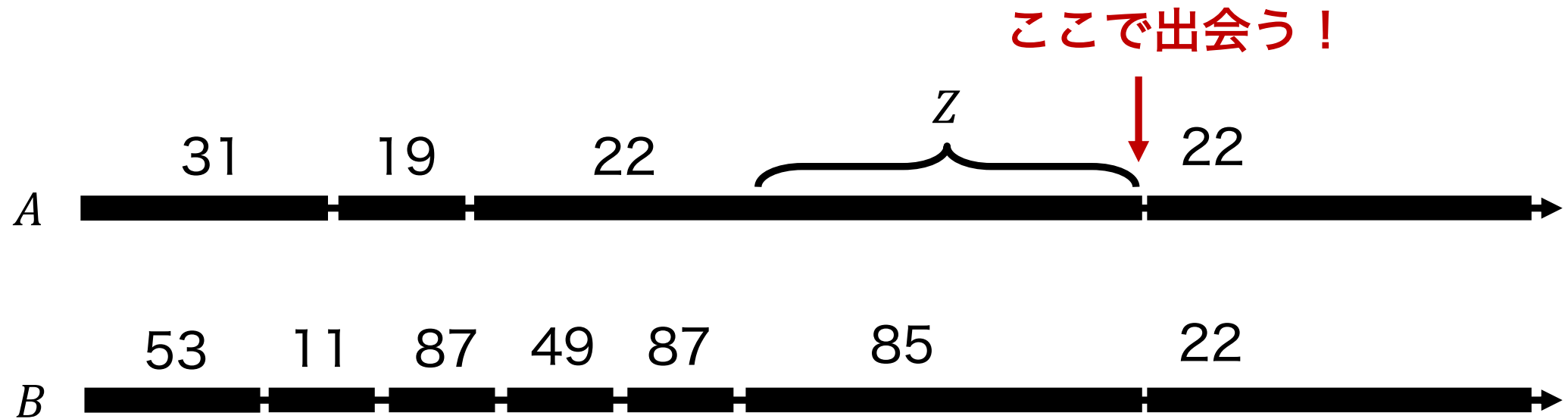
N : 頂点数 n の上界 ($n = O(N)$ を仮定) 、 f : 悪性エー
ジェント数、
 F : 悪性エー
ジェント数 f の上界、 K : エー
ジェント数 k の上界、
 α : $\log K$ 以上の任意の整数

Dieudonnéら [3]のアルゴリズム

- TZ法をサブルーチンとして活用
 - 集団IDを ℓ としたときのTZ法を $TZ(\ell)$ と表記
- 正常エージェントは集団IDとして変数 ℓ を管理
 - 各時刻でエージェントは $TZ(\ell)$ を実行
 - $TZ(\ell)$ は $Z = O(X(n) \cdot \lambda)$ 時間で終わるが、終わり次第、最初から $TZ(\ell)$ を実行
 - 変数 ℓ は他エージェントとの合流や別離により変化する（後述）

TZ法が保証してくれること

- 2つの集団A,Bが異なる整数 ℓ_A, ℓ_B に対しそれぞれ $TZ(\ell_A), TZ(\ell_B)$ を実行しつづけると、 $Z = O(X(n) \cdot \lambda)$ 時間以内に2つの集団は出会う



$TZ(\ell)$ の開始時刻のずれは問題にならない

集団ID ℓ の管理と $TZ(\ell)$ の初期化

- 離れた集団が確実に出会えるよう、
各集団は**集団内に実在するエージェントのID**を集団IDとする
- 具体的には...
各エージェントは、同一頂点に存在するエージェントのうち
ブラックリストに含まれないエージェント群を自集団とし、
自集団に属すエージェントの最小IDを集団IDとする
 - 一度合流した正常エージェントは二度と離別させたくない
→ **同一頂点に存在する正常エージェントは
全員同じブラックリストを持つ**ように工夫する（**超重要！**）
- 自集団を構成するエージェントの集合に変化があった場合には
（集団ID ℓ の更新有無に関わらず） $TZ(\ell)$ を更新する

ブラックリストの管理[3]

Definition 3.1. If $MyGroup_a(t) = \emptyset$, then $BlackList_a(t) = \emptyset$. Otherwise, $BlackList_a(t)$ is the set $B \subset MyGroup_a(t)$ of largest size such that for all $\alpha' \in B$ there exist $t' < t'' \leq t$ satisfying the following three properties:

- (1) $MyGroup_a(t) \setminus B \subseteq MyGroup_a(t') \setminus B$
- (2) $MyGroup_a(t) \setminus B \subseteq MyGroup_a(t'') \setminus B$
- (3) $\alpha' \in MyGroup_a(t') \setminus MyGroup_a(t'')$

ブラックリストの管理[3]

Definition 3.1. If $MyGroup_a(t) = \emptyset$, then $BlackList_a(t) = \emptyset$. Otherwise, $BlackList_a(t)$ is the set $B \subset MyGroup_a(t)$ of largest size such that for all $\alpha' \in B$ there exist $t' < t'' \leq t$ satisfying the following three properties:

- (1) $MyGroup_a(t) \setminus B \subseteq MyGroup_a(t') \setminus B$
- (2) $MyGroup_a(t) \setminus B \subseteq MyGroup_a(t'') \setminus B$
- (3) $\alpha' \in MyGroup_a(t') \setminus MyGroup_a(t'')$

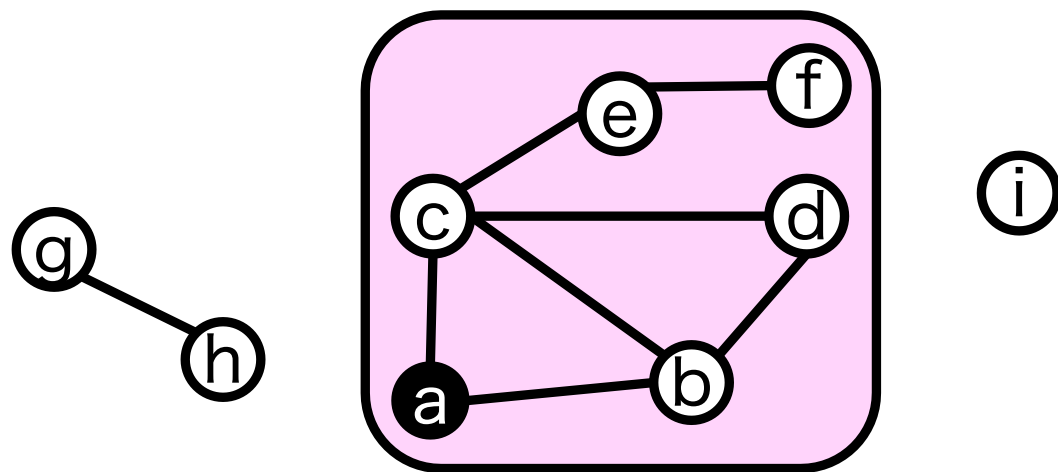
ややこしい！！！！

ブラックリストの管理法 (噛み砕いた定義 1/2)

- どのエージェントも他エージェントの正常性を確信できない
 - どれだけ長い時間をかけても
 - 悪性エージェントは永続的に正常エージェントと同じ動作をするかもしれない
- 一方で、正常エージェントは
悪性エージェントのあきらかに悪的な動作を直接観測することがある
 - 同じ集団IDで $TZ(\ell)$ を実行しているのに突然いなくなる、など
- エージェント a がエージェント b の悪性動作を未観測であるとき、
 a は b を信用しているという
 - 正常かどうかは分からないが悪性とは断定できない、くらいの意味

ブラックリストの管理法 (噛み砕いた定義 2/2)

- 信用グラフ $G_{v,t} = (V_{v,t}, E_{v,t})$
 - 頂点集合 $V_{v,t} =$ (時刻 t で頂点 v に存在するエージェントの集合)
 - 辺集合 $E_{v,t} = \{\{a, b\} \in V_{v,t} \mid a, b \text{ は時刻 } t \text{ で相互に信用している}\}$



- 時刻 t で頂点 v に存在するエージェント a のブラックリスト $B_{a,t}$:
信用グラフ $G_{v,t}$ において
 a を含む連結成分に含まれないエージェントの集合

嬉しい3つの補題

k : エージェント数
 f : 悪性エージェント数

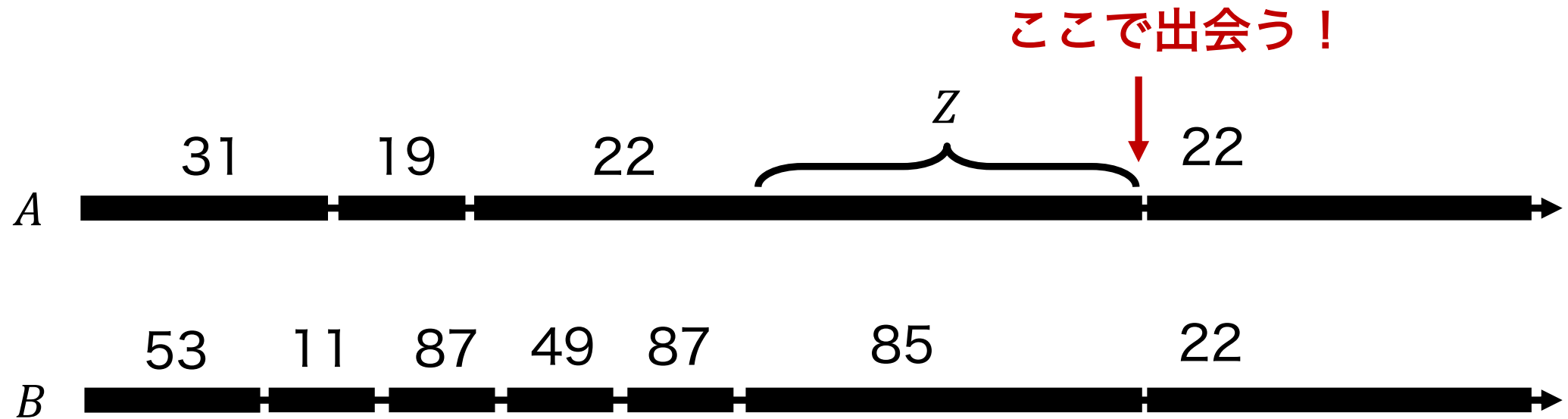
補題1 [3] :
任意の2つの正常エージェントは、
同一頂点上に位置するとき同じブラックリストを持つ

補題2 [3] :
任意の2つの正常エージェントは一度合流すると以後離れない
(i.e, 常に一緒に移動する)

補題3 [3] :
どの正常エージェントも高々 $2kf$ 回しか自集団が変化しない

(再掲) TZ法が保証してくれること

- 2つの集団A,Bが異なる整数 ℓ_A, ℓ_B に対しそれぞれ $TZ(\ell_A), TZ(\ell_B)$ を実行しつづけると、 $Z = O(X(n) \cdot \lambda)$ 時間以内に2つの集団は出会う



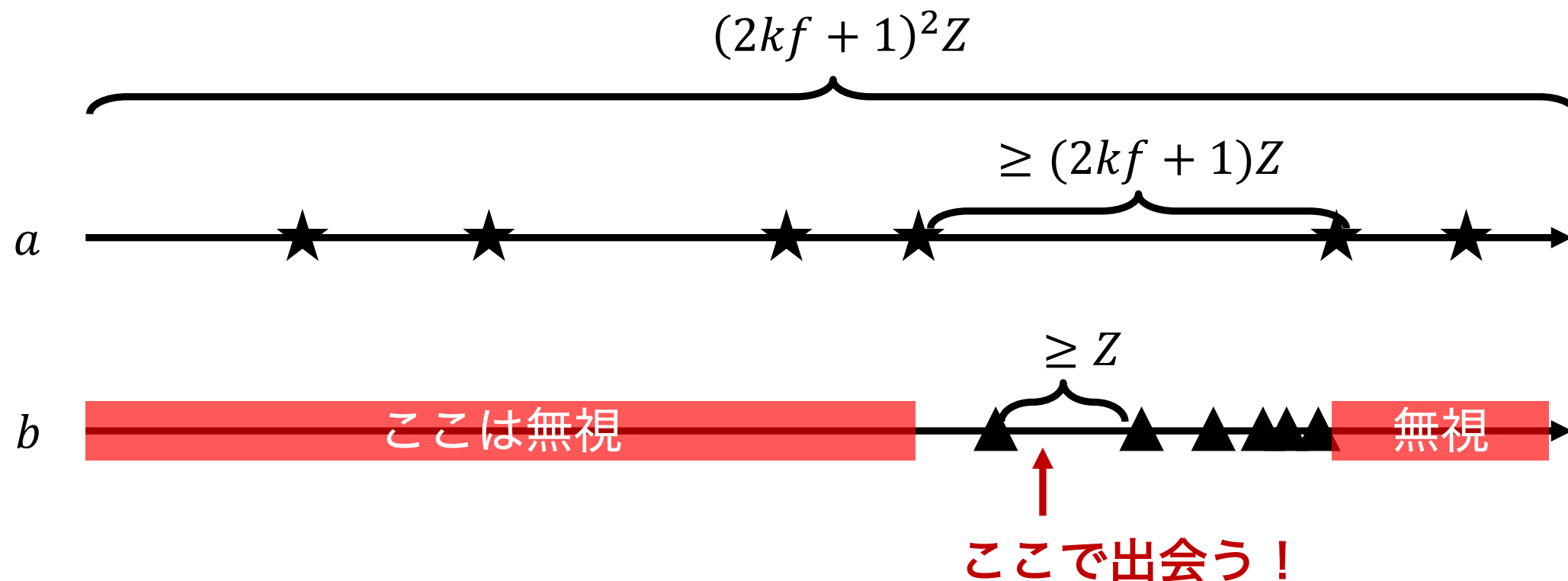
$TZ(\ell)$ の開始時刻のずれは問題にならない

計算量解析のコアとなる補題

★ : a の集団が変化する時刻
▲ : b の集団が変化する時刻

補題4 [3] :

任意の2つの正常エージェント a, b は $(2kf + 1)^2 \cdot Z$ 時間以内に出会う



正当性・時間計算量の証明

補題4（再掲）：

任意の2つの正常エージェント a, b は $(2kf + 1)^2 \cdot Z$ 時間以内に出会う

系1：

時刻 $(2kf + 1)^2 \cdot Z$ にすべての正常エージェントは同一の頂点に滞在

時刻 $(2kf + 1)^2 \cdot Z$ に各エージェントが停止することとすると…

定理1：

Dieudonnéら[3]のアルゴリズムは

ビザンチン集合問題を $O(k^2 f^2 X(n) \lambda)$ 時間で解く

ビザンチン集合アルゴリズム

	初期知識	悪性エージェント数の制約	白板	署名	時間計算量	成功率
Dieudonnéら[3]	N	なし	なし	なし	$O(k^2 f^2 \lambda \cdot X(n))$	1
鈴木・首藤	N	なし	なし	なし	$O(kf\lambda \cdot X(n))$	1
Hiroseら[4]	N	$f = O(\sqrt{k})$	なし	なし	$O((f + \lambda) \cdot X(n))$	1
Hiroseら[5]	N, F	$F \leq (k - 1)/3$	なし	なし	$O(F\lambda \cdot X(n))$	1
Hiroseら[5]	N	$f \leq (k - 1)/9$	なし	なし	$O(f\lambda \cdot X(n))$	1
Tsuchidaら[6]	F	なし	あり	あり	$O(Fm)$	1
小杉・首藤	K	なし	あり	なし	$O(m + \alpha n K)$	$1 - 1/2^\alpha$

N : 頂点数 n の上界 ($n = O(N)$ を仮定) 、 f : 悪性エージェント数、
 F : 悪性エージェント数 f の上界、 K : エージェント数 k の上界、
 α : $\log K$ 以上の任意の整数

Dieudonnéら[3]のアルゴリズムの鈴木らの改良

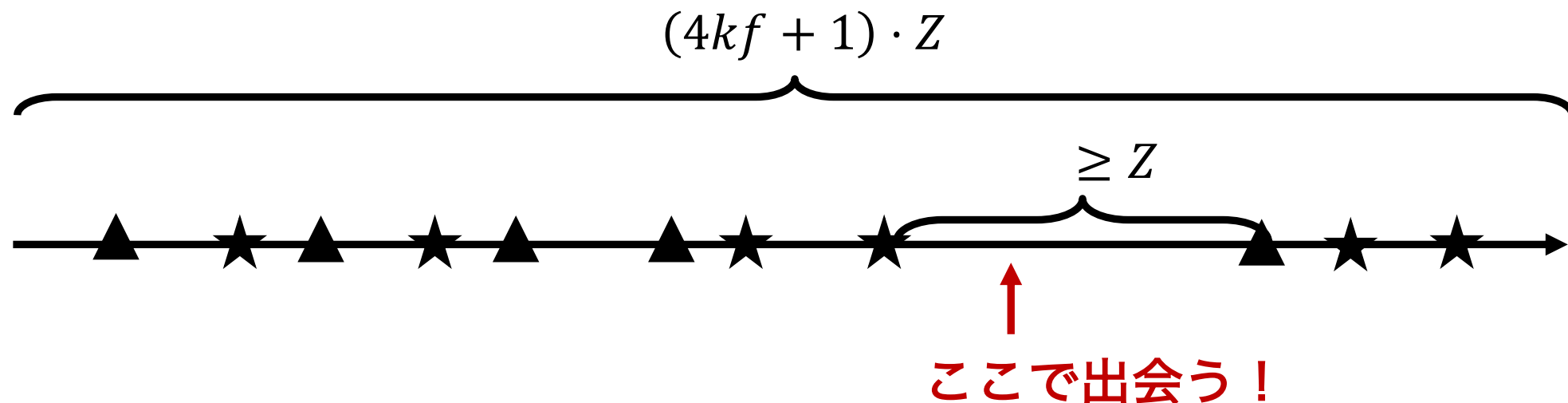
- Dieudonnéら[3]のアルゴリズムは
悪性エージェント数の制約がない集合アルゴリズムとして
現時点でstate of artであり、多くの論文に引用され、比較され、
またサブルーチンとして利用されている
- ただし、なぜか正常エージェントが出会うまで時間の解析が
極めて甘いことを誰も指摘してこなかった
- 鈴木らはこの部分をきちんと解析したことによって
Dieudonnéら[3]のアルゴリズムの時間計算量を $1/kf$ 倍に改良した

計算量解析のコアとなる補題

★ : a の集団が変化する時刻
▲ : b の集団が変化する時刻

補題4改 :

任意の2つの正常エージェント a, b は $(4kf + 1) \cdot Z$ 時間以内に出会う



正当性・時間計算量の証明

補題4改（再掲）：

任意の2つの正常エージェント a, b は $(4kf + 1) \cdot Z$ 時間以内に出会う

系1改：

時刻 $(4kf + 1) \cdot Z$ にすべての正常エージェントは同一の頂点に滞在

時刻 $(4kf + 1) \cdot Z$ に各エージェントが停止することとすると…

定理1改：

改良版Dieudonnéら[3]のアルゴリズムは

ビザンチン集合問題を $O(kfX(n)\lambda)$ 時間で解く

まとめ

	初期知識	悪性エージェント数の制約	白板	署名	時間計算量	成功率
Dieudonnéら[3]	N	なし	なし	なし	$O(k^2 f^2 \lambda \cdot X(n))$	1
鈴木・首藤	N	なし	なし	なし	$O(\mathbf{k} \mathbf{f} \lambda \cdot X(n))$	1
Hiroseら[4]	N	$f = O(\sqrt{k})$	なし	なし	$O((f + \lambda) \cdot X(n))$	1
Hiroseら[5]	N, F	$F \leq (k - 1)/3$	なし	なし	$O(F \lambda \cdot X(n))$	1
Hiroseら[5]	N	$f \leq (k - 1)/9$	なし	なし	$O(f \lambda \cdot X(n))$	1
Tsuchidaら[6]	F	なし	あり	あり	$O(Fm)$	1
小杉・首藤	K	なし	あり	なし	$\mathbf{O}(m + \alpha n K)$	$\mathbf{1 - 1/2^\alpha}$

N : 頂点数 n の上界 ($n = O(N)$ を仮定) 、 f : 悪性エージェント数、
 F : 悪性エージェント数 f の上界、 K : エージェント数 k の上界、
 α : $\log K$ 以上の任意の整数