Bizantyńscy generałowie: zdrada, telekomunikacja i fizyka

P. F. Góra

Wydział Fizyki, Astronomii i Informatyki Stosowanej UJ

26 września 2018

Co to jest fizyka?

Nauka o otaczającym nas świecie

Co to jest fizyka?

Nauka o otaczającym nas świecie

- chemia?
- biologia?
- geologia?
- . . . ?

Co to jest fizyka?

Nauka o otaczającym nas świecie

- chemia?
- biologia?
- geologia?
- . . . ?

Fizyka to to, czym zajmują się fizycy ☺

Co charakteryzuje fizykę?

Co charakteryzuje fizykę?

- wyidealizowane modele matematyczne
  - punkt materialny, bryła sztywna, funkcja falowa, bispinor, . . .

Co charakteryzuje fizykę?

- wyidealizowane modele matematyczne
  - punkt materialny, bryła sztywna, funkcja falowa, bispinor, . . .
- oddziaływania
  - siły (fizyka “szkolna” i “techniczna”)
  - pola sił (fizyka klasyczna i kwantowa)
  - wymiana wirtualnych cząstek (kwantowa teoria pola)

Bez oddziaływań nie ma fizyki!

Oddziaływania to wymiana informacji

Cząstka X dowiaduje się o stanie innej cząstki Y lub o stanie swojego otoczenia i na tej podstawie zmienia parametry swojego ruchu lub swój stan wewnętrzny. Informacja na ogół jest zwrotna (jeśli cząstka X dowiaduje się o cząstce Y, to cząstka Y dowiaduje się o cząstce X): trzecia zasada dynamiki Newtona.

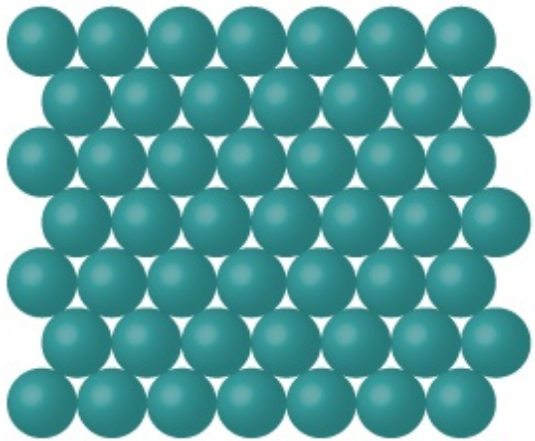
Oddziaływania to wymiana informacji

Cząstka X dowiaduje się o stanie innej cząstki Y lub o stanie swojego otoczenia i na tej podstawie zmienia parametry swojego ruchu lub swój stan wewnętrzny. Informacja na ogół jest zwrotna (jeśli cząstka X dowiaduje się o cząstce Y, to cząstka Y dowiaduje się o cząstce X): trzecia zasada dynamiki Newtona.
Przykład: Cząstka o masie m_1, ładunku q_1, pędzie $\vec{p}_1$ i położeniu $\vec{r}_1$ dowiaduje się

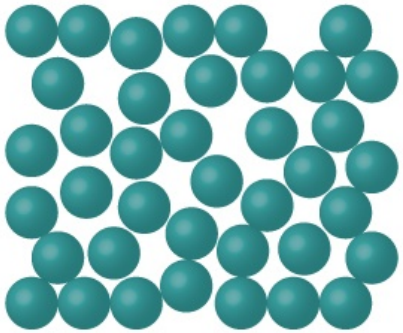
- za pośrednictwem pola elektromagnetycznego (elektrodynamika klasyczna)
- za pośrednictwem wirtualnych fotonów (elektrodynamika kwantowa)

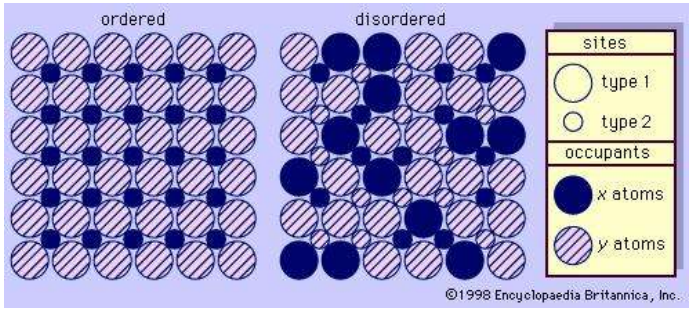
o cząstce o masie m_2, ładunku q_2, pędzie $\vec{p}_2$ i położeniu $\vec{r}_2$ i *vice versa*. Na skutek tej wymiany informacji obie cząstki zmieniają swój ruch zgodnie z równaniami elektrodynamiki.

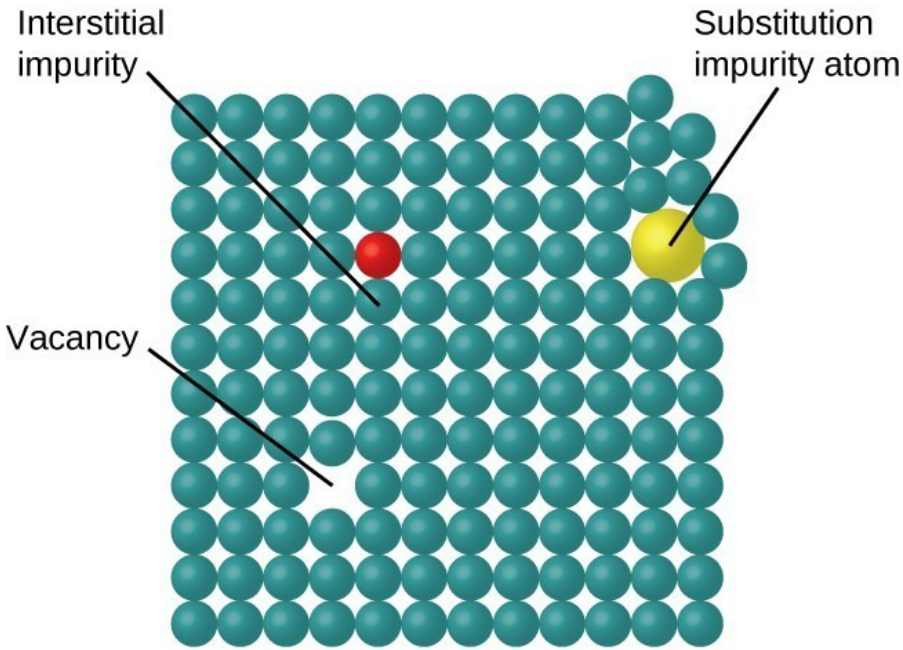
Informacja może docierać do cząstki z jakiegoś układu uporządkowanego, o znanej strukturze...



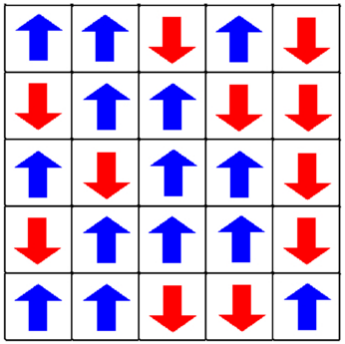
. . . lub nieuporządkowanego







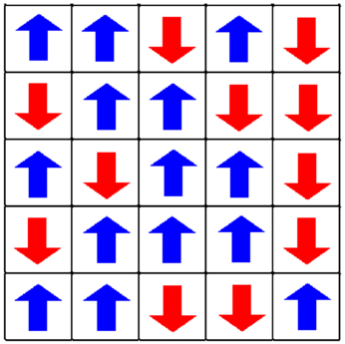
Stan układu może być zmienny w czasie, także losowo



strzałki “obracają się” w wyniku rzutu monetą albo jakiegoś bardziej skomplikowanego procesu losowego, na przykład ruchów cieplnych.

Prowadzi to do badania układów nieuporządkowanych i losowo (stochastycznie) zmiennych w czasie.

Stan układu może być zmienny w czasie, także losowo



strzałki “obracają się” w wyniku rzutu monetą albo jakiegoś bardziej skomplikowanego procesu losowego, na przykład ruchów cieplnych.

Prowadzi to do badania układów nieuporządkowanych i losowo (stochastycznie) zmiennych w czasie. Gdyby fizyka nie nauczyła się badać i modelować takich układów, **nie mielibyśmy** — na przykład — układów półprzewodnikowych, a zatem komputerów, smartfonów, nowoczesnych telewizorów, satelitów telekomunikacyjnych i Internetu

☹

Możemy nie znać stanu jakiegoś układu fizycznego

Możemy nie znać stanu jakiegoś układu fizycznego , ale układy fizyczne nigdy nie kłamią na temat swojego stanu.

Możemy nie znać stanu jakiegoś układu fizycznego , ale układy fizyczne nigdy nie kłamią na temat swojego stanu.

Czy coś w przyrodzie może kłamać?!

Sieć komputerowa

Sieć komputerowa

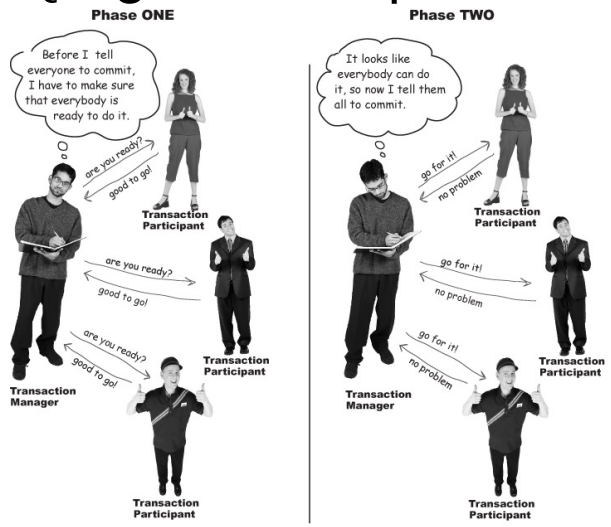
- Co się stanie, gdy jeden z komputerów się popsuje?

Sieć komputerowa

- Co się stanie, gdy jeden z komputerów się popsuje?
- Co się stanie, gdy jeden z komputerów się popsuje, a my nie będziemy o tym wiedzieli?!

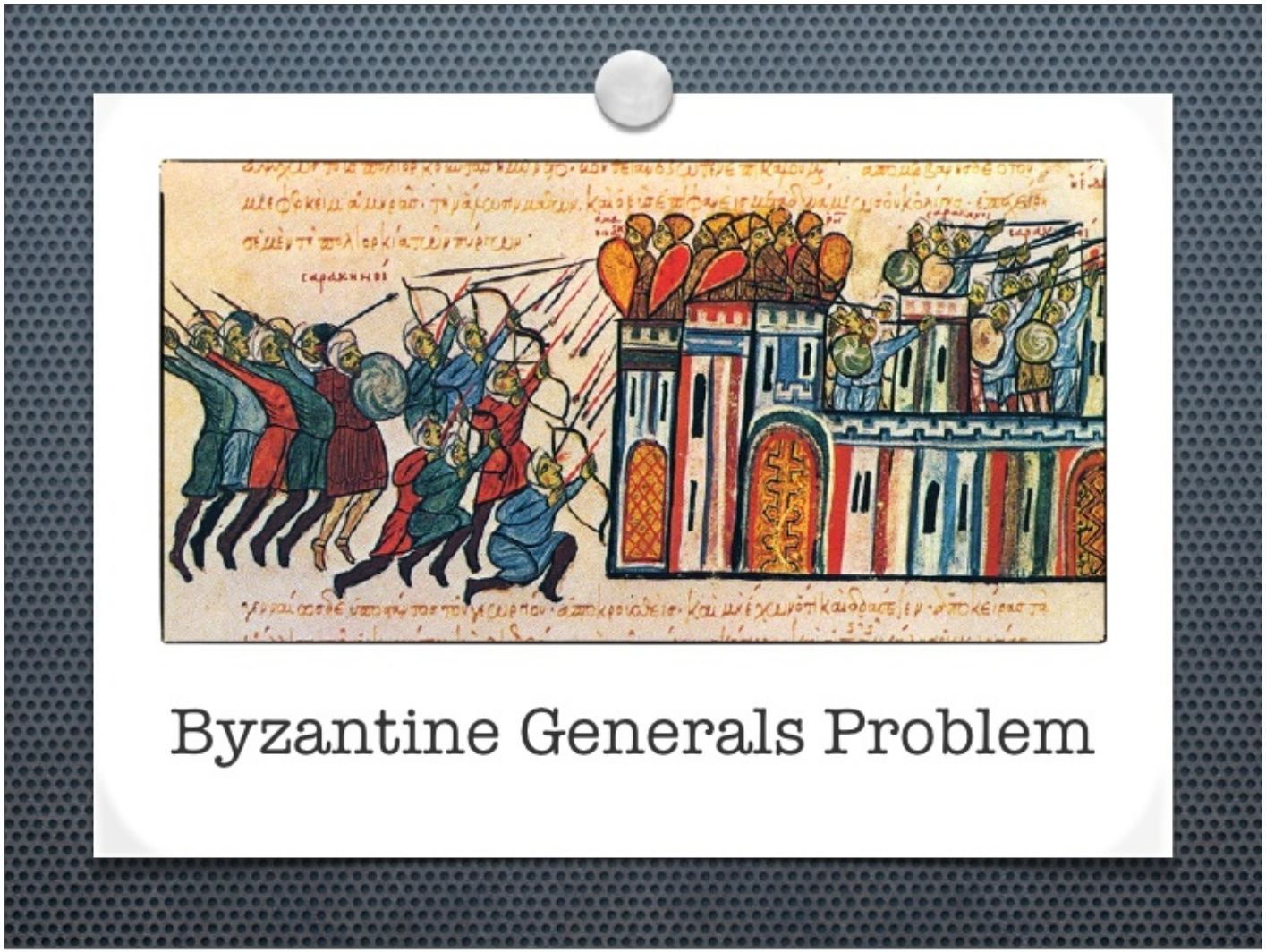
Protokół Two-Phase Commit

Wszystkie komputery w sieci muszą się zgodzić na pewne działanie

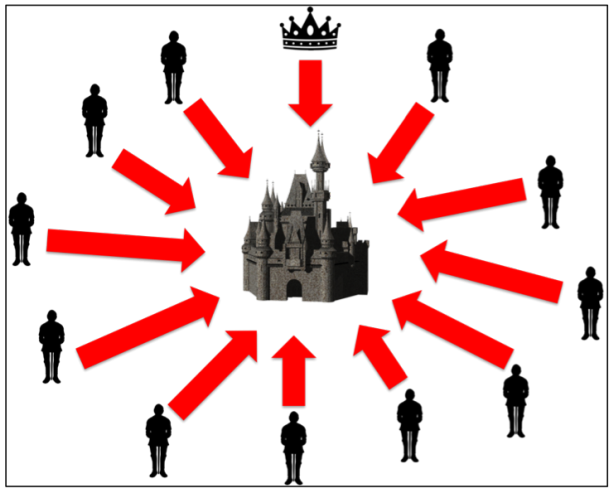


Jeśli któryś się nie zgodzi lub nie odpowie w określonym czasie, operacja zostaje odwołana

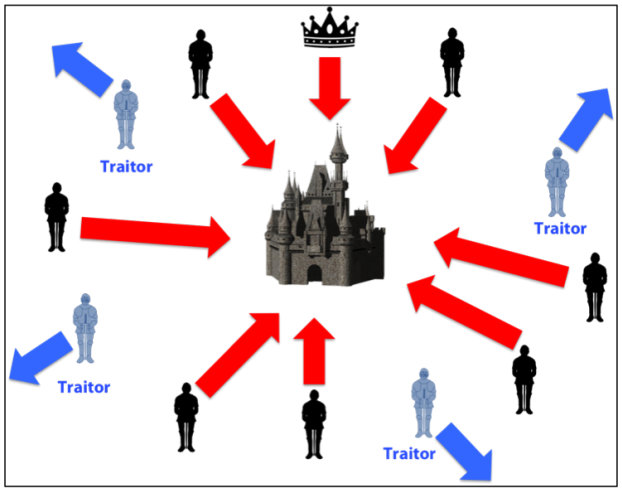
A jeśli ktoś oszukuje?!



Kilka bizantyńskich armii oblega miasto. Tylko skoordynowany atak lub skoordynowany odwrót zapewnia sukces. Jeśli część armii zaatakuje, część się wycofa, wszystkie armie poniosą porażkę. Generałowie wymieniają (przez posłańców) informacje aby uzgodnić wspólną strategię.

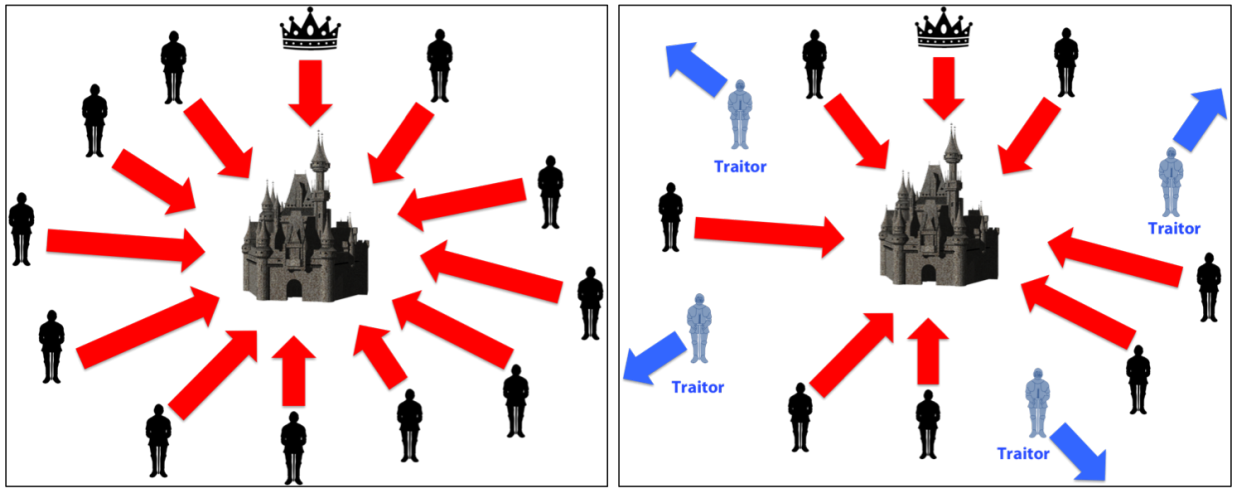


Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

Kilka bizantyńskich armii oblega miasto. Tylko skoordynowany atak lub skoordynowany odwrót zapewnia sukces. Jeśli część armii zaatakuje, część się wycofa, wszystkie armie poniosą porażkę. Generałowie wymieniają (przez posłańców) informacje aby uzgodnić wspólną strategię.



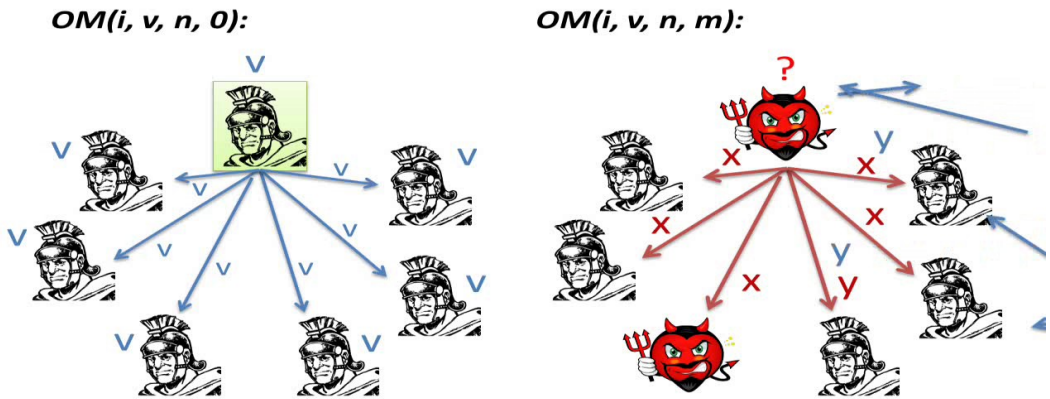
Coordinated Attack Leading to Victory Uncoordinated Attack Leading to Defeat

Problem: wśród generałów mogą być zdrajcy, którzy fałszywie informują o swoich zamiarach.

W języku sieci komputerowych: Czy uda się uzgodnić *zadowalające* rozwiązanie, jeśli pewna liczba komputerów działa nieprawidłowo (awaria, atak hakerów)?

A Solution with Oral Messages

($n \geq 3m + 1$)



Klasyczne rozwiązanie: Ponad 2/3 komputerów musi działać prawidłowo.

Gdzie to ma zastosowanie?

- sieci komputerowe i telekomunikacyjne, w szczególności
- rozproszone bazy danych i rozproszone systemy obliczeniowe,
- Blockchain[1] (Bitcoin i inne waluty),
- Internet Rzeczy (IoT) i “Smart Contracts”

[1] Rozproszony, zdecentralizowany (bez centralnej jednostki autoryzującej) system zapewniania zaufania.

Fizyka to to, czym zajmują się fizycy ☺

Badanie i modelowanie układów “niefizycznych” metodami wywodzącymi się z fizyki

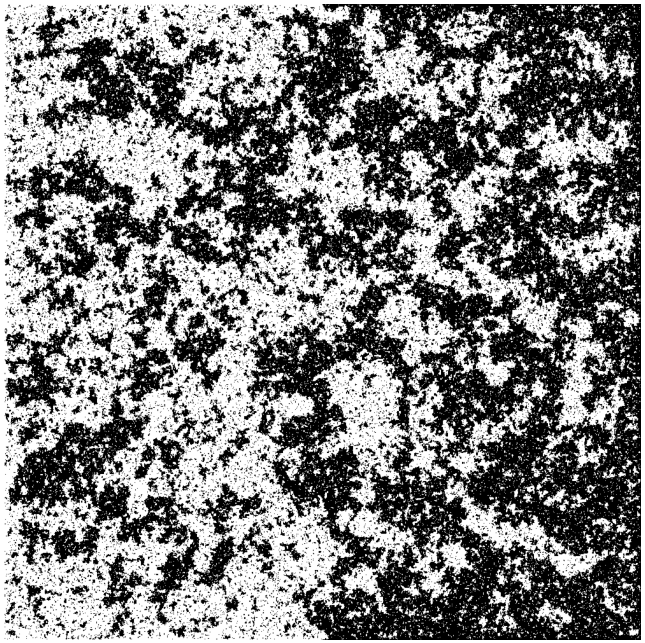
Fizyka to to, czym zajmują się fizycy ☺

Badanie i modelowanie układów “niefizycznych” metodami wywodzącymi się z fizyki

Na przykład:

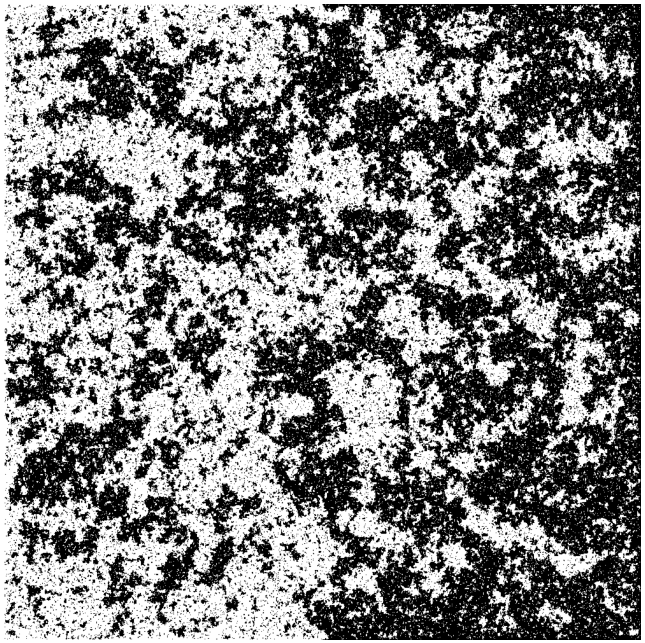
- Ekonofizyka
- Socjofizyka
- Badanie sieci społecznych, troficznych, ekspresji genów, a także telekomunikacyjnych tak, jakby były to układy “krystaliczne”

Przykład:



Model dwuwymiarowego kryształu magnetycznego na granicy przejścia paramagnetyk-ferromagnetyk.

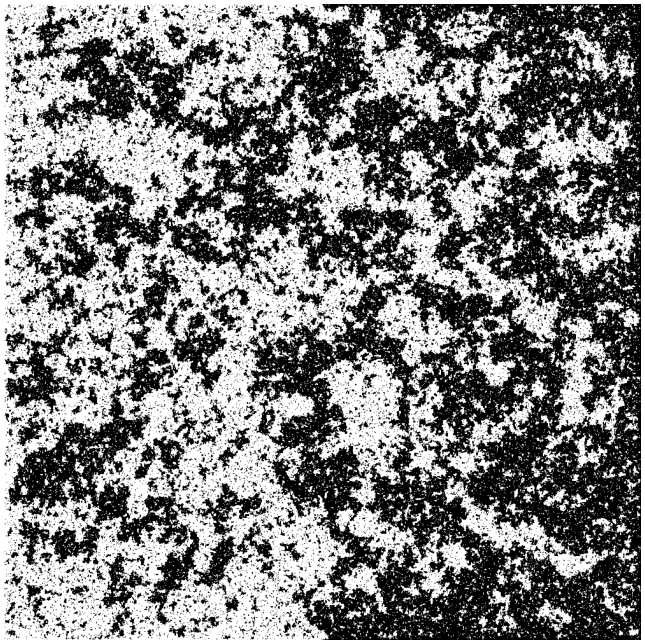
Przykład:



Model dwuwymiarowego kryształu magnetycznego na granicy przejścia paramagnetyk-ferromagnetyk.

A może model rozprzestrzeniania się epidemii?

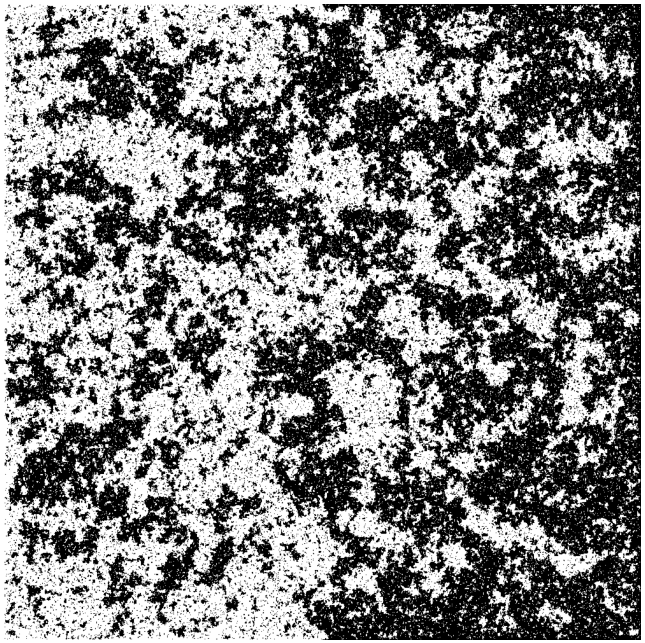
Przykład:



Model dwuwymiarowego kryształu magnetycznego na granicy przejścia paramagnetyk-ferromagnetyk.

A może model rozprzestrzeniania się epidemii? Model pożaru lasu?

Przykład:



Model dwuwymiarowego kryształu magnetycznego na granicy przejścia paramagnetyk-ferromagnetyk.

A może model rozprzestrzeniania się epidemii? Model pożaru lasu?
Model rozprzestrzeniania się opinii lub preferencji wyborczych?

Inny przykład:

Modele “agentowe”: Elementy układu (“agenci”) podejmują decyzje — na przykład o zakupie akcji — na podstawie zachowań (stanu) innych agentów, których obserwują. Dodatkowo uwzględnia się zaburzenia losowe.

Inny przykład:

Modele “agentowe”: Elementy układu (“agenci”) podejmują decyzje — na przykład o zakupie akcji — na podstawie zachowań (stanu) innych agentów, których obserwują. Dodatkowo uwzględnia się zaburzenia losowe.

Rozważa się modele, w których informacja uzyskiwana z otoczenia jest niepewna, rozmyta.

Inny przykład:

Modele “agentowe”: Elementy układu (“agenci”) podejmują decyzje — na przykład o zakupie akcji — na podstawie zachowań (stanu) innych agentów, których obserwują. Dodatkowo uwzględnia się zaburzenia losowe.

Rozważa się modele, w których informacja uzyskiwana z otoczenia jest niepewna, rozmyta.

Ale w takich modelach niektórzy “agenci” mogą kłamać, zachowywać się jak bizantyńscy zdrajcy, aby ich rywale podjęli *niekorzystne* decyzje.

Inny przykład:

Modele “agentowe”: Elementy układu (“agenci”) podejmują decyzje — na przykład o zakupie akcji — na podstawie zachowań (stanu) innych agentów, których obserwują. Dodatkowo uwzględnia się zaburzenia losowe.

Rozważa się modele, w których informacja uzyskiwana z otoczenia jest niepewna, rozmyta.

Ale w takich modelach niektórzy “agenci” mogą kłamać, zachowywać się jak bizantyńscy zdrajcy, aby ich rywale podjęli *niekorzystne* decyzje.

Jeszcze inny przykład: Optymalizacja wielowymiarowa (stosowana na przykład w *Deep Learning*) — niektóre stany mogą kłamliwie raportować wartość funkcji dopasowania.

Fizyka łączy doświadczenie i metody z układów nieuporządkowanych i stochastycznych z metodami zaczerpniętymi z informatyki, takimi jak problem bizantyńskich generałów, aby uzyskać wyniki nieznane dotąd ani fizyce, ani informatyce, ani innym naukom szczegółowym.

Otwierają się zupełnie nowe obszary badawcze ☺