Universität Zürich[UZH]

Blockchain & Distributed Ledger Technologies

UZH Blockchain Center

Percolation and Robustness

Lecture 8

Claudio J. Tessone

Blockchain & Distributed Ledger Technologies
UZH Blockchain Center

Lecture Objectives

1. Understand the effect of deterioration of the network
2. Learn the different approaches to study network percolation and robustness
3. Learn the basic models for cascading failures

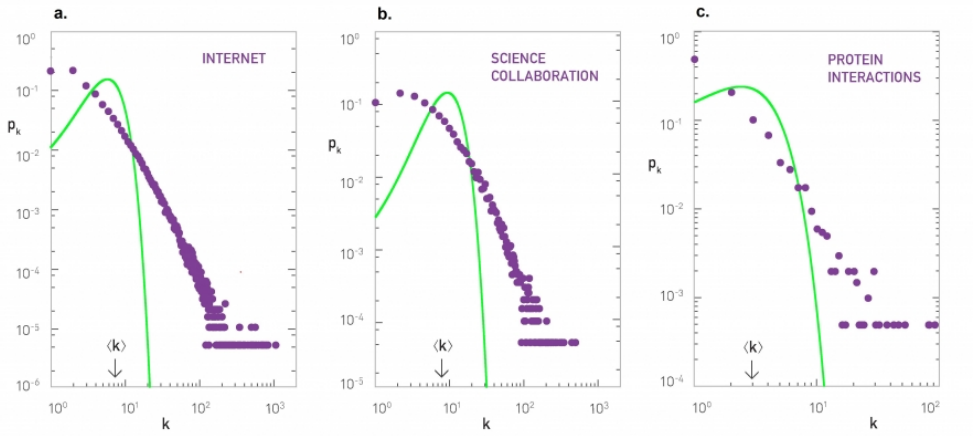
So far, we have looked into network structure and its most common network properties

What about network function?

If nodes fail or edges get broken... are the functions of the system preserved?

Contents

Scale-Free networks



Real networks have many low degree nodes but also hubs

Degree distributions does not have a characteristic scale

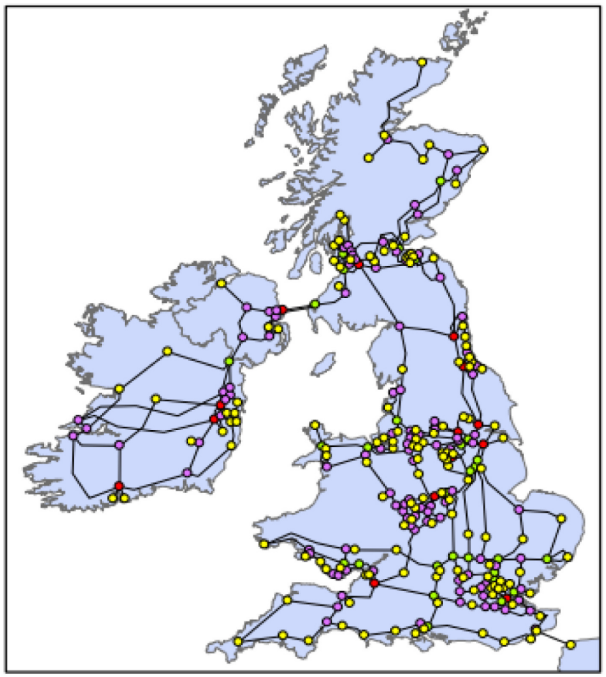
Power-law degree distribution $P(k) \sim k^{-\gamma}$

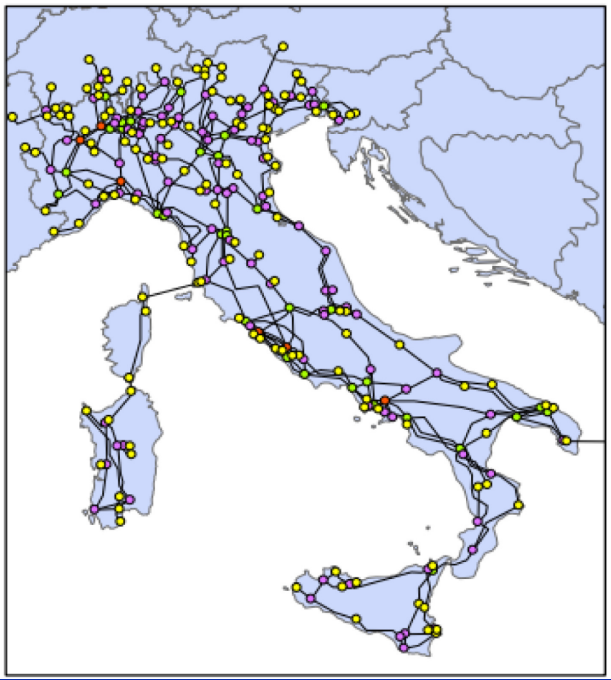
Percolation Theory

Robustness in applications

- **Biology and medicine**: helps understand why some mutations lead to diseases and others do not;
- **Economics**: explores economic stability against cascade of failures (e.g. of financial institutions or interruptions in chain of payments)
- **Environmental science**: predicts failure of an ecosystem when facing exogenous disruptions (e.g. human activity)
- **Engineering**: transport or distribution systems that must sustain basic functions

Power grids

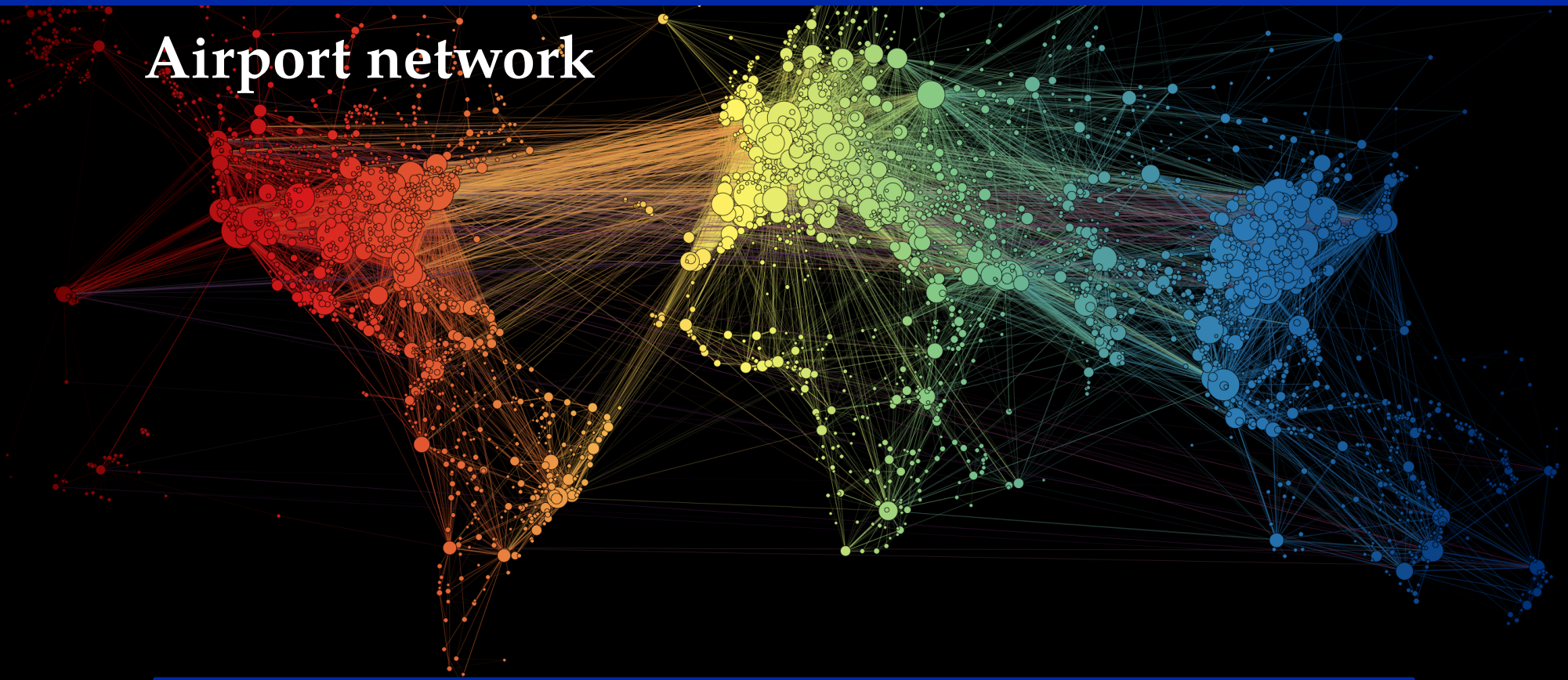




Nodes can be generators / distribution stations, links electrical connection

What happens if nodes fail? What happens if transmision lines fail?

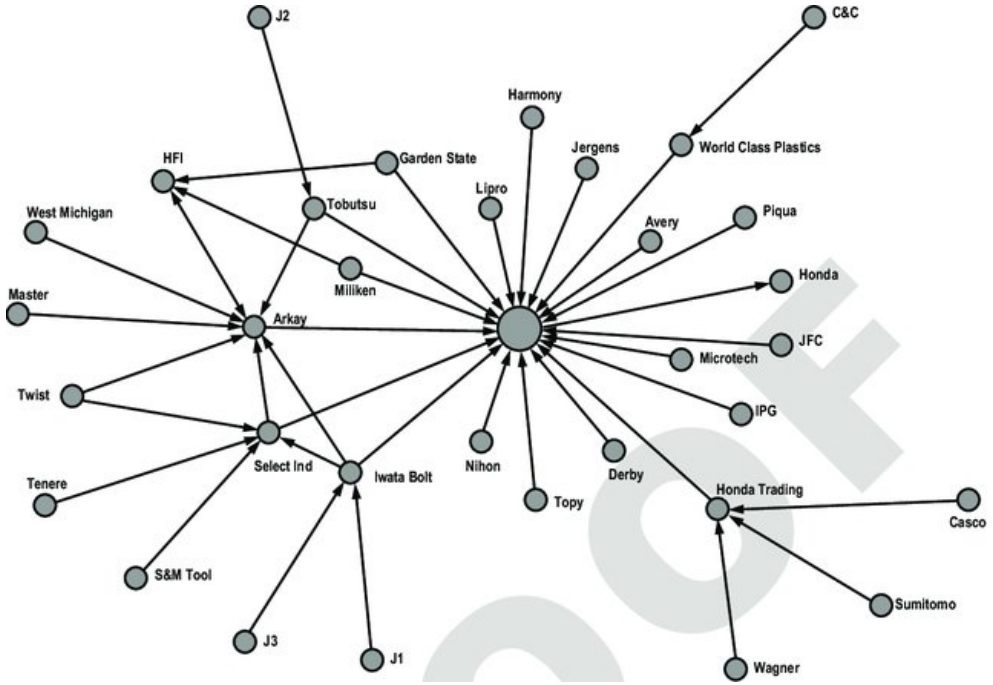
Airport network



Nodes are airports, links are air routes between them

What happens in case of airport disruption? What happens if an airline goes bankrupt?

Supply chain network

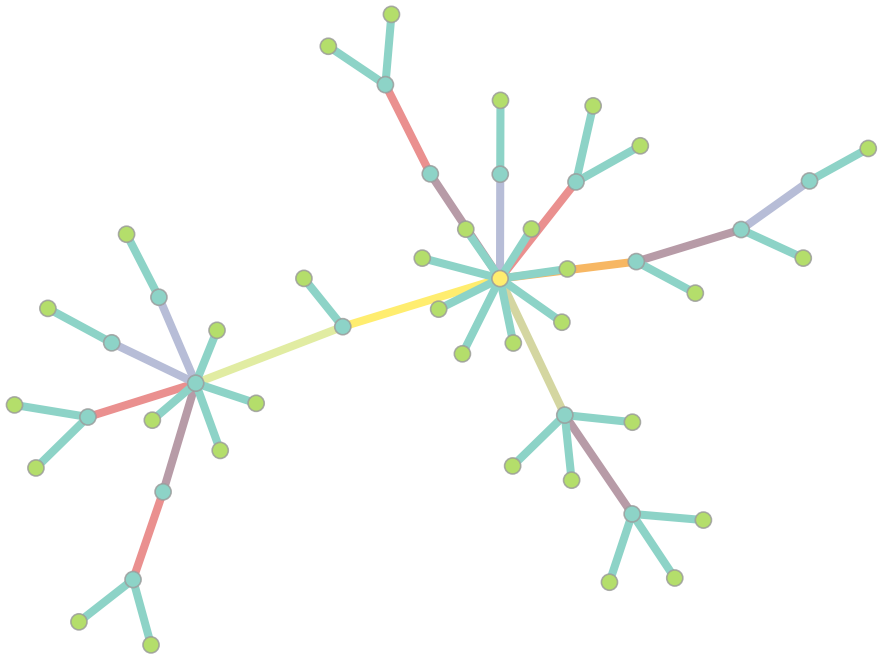


Nodes are companies in the distribution, links are flow of goods

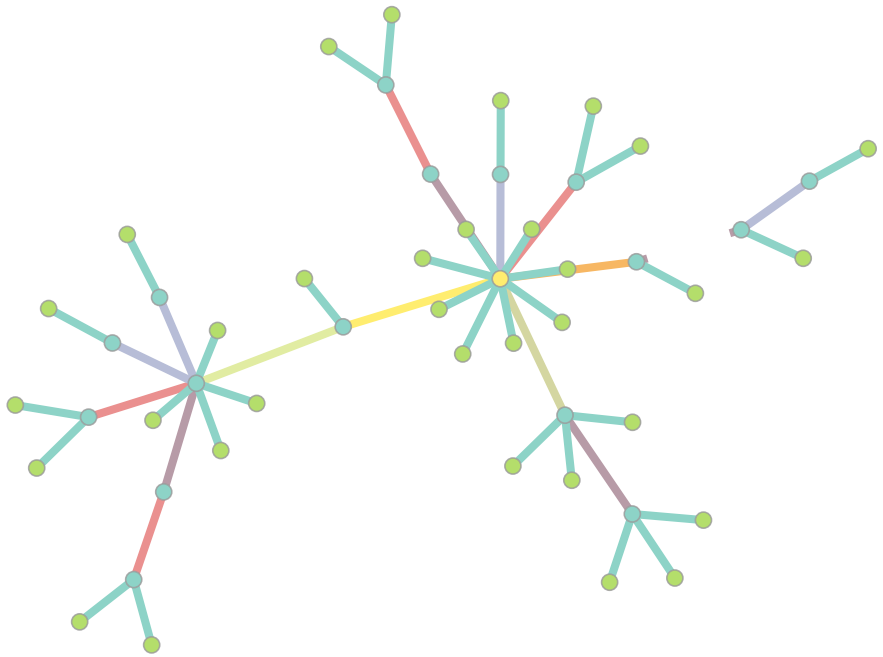
What happens when a company cannot deliver the products needed down the line?

Percolation theory

What is percolation?

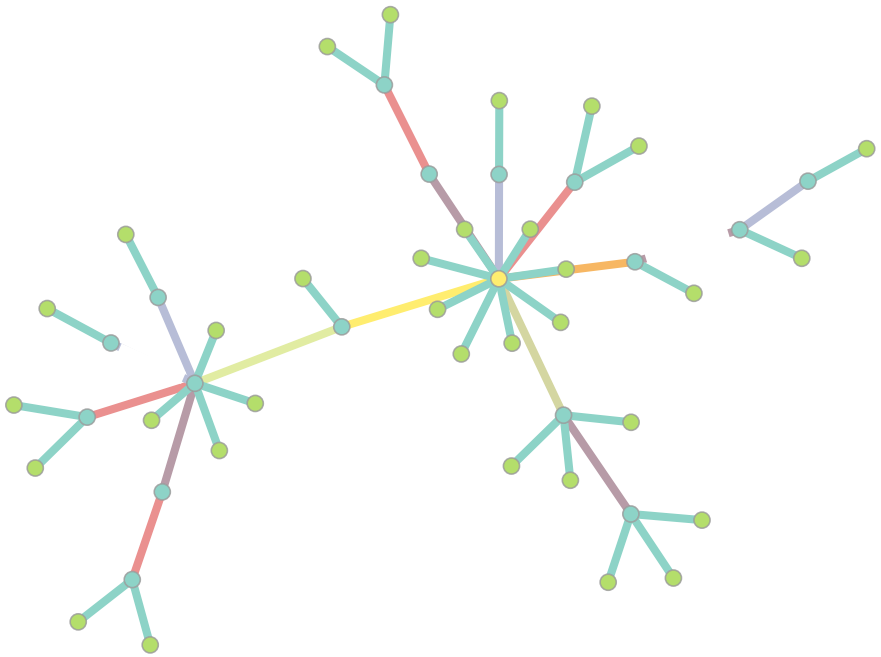


What is percolation?



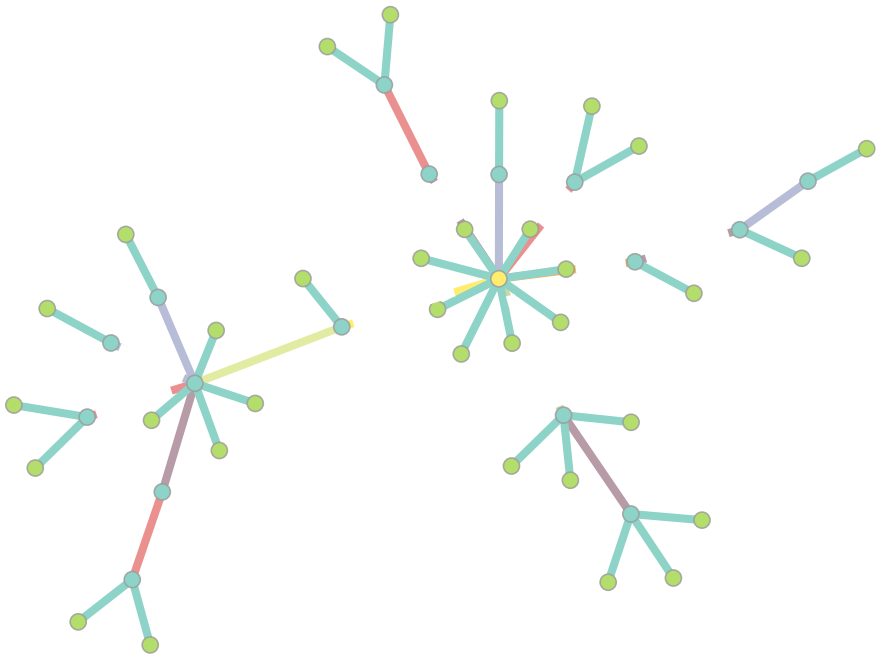
How many nodes can we remove while the network preserves its functioning condition?

What is percolation?



How many nodes do we need to remove to fragment the network into isolated components?

What is percolation?



How many nodes do we need to remove to fragment the network into isolated components?

An historical introduction to percolation

Percolation on 2D lattice

- Suppose a node exists on every intersection with probability p
- Edges connect neighbouring nodes in the lattice

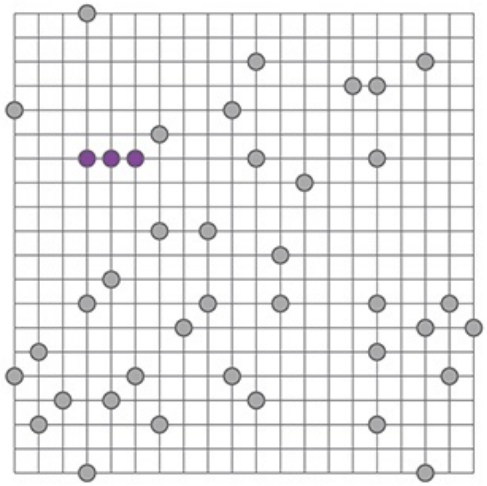
A cluster is a set of nodes reachable from each other

Percolation on 2D lattice

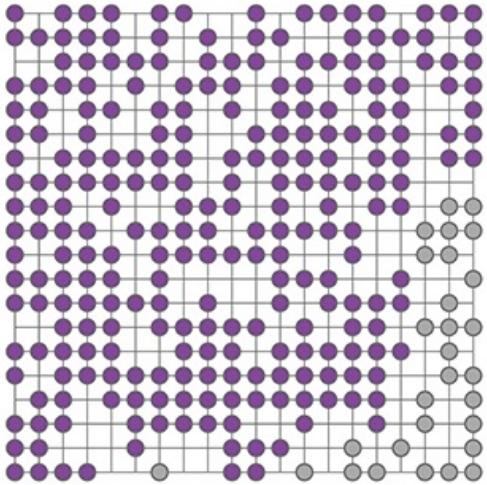
- Suppose a node exists on every intersection with probability p
- Edges connect neighbouring nodes in the lattice

A cluster is a set of nodes reachable from each other

a. p = 0 .1



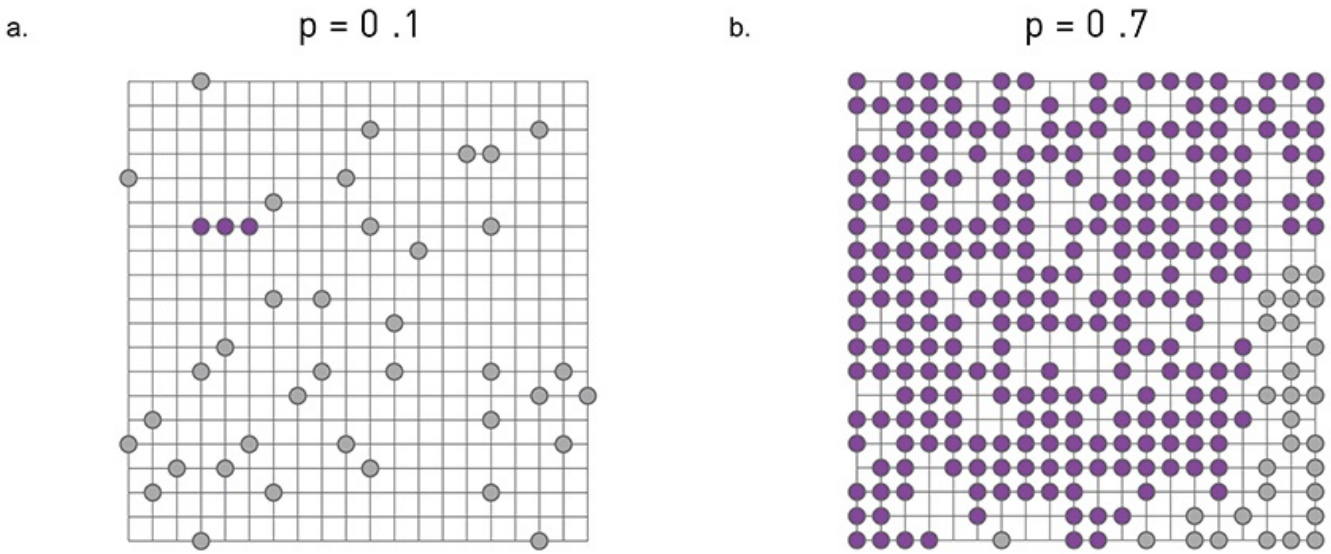
b. p = 0 .7



Percolation on 2D lattice

- A percolating cluster is one such that it reaches both (left-right) ends of the lattice

At what critical probability p_c exists a percolating cluster?



Percolation on 2D lattice

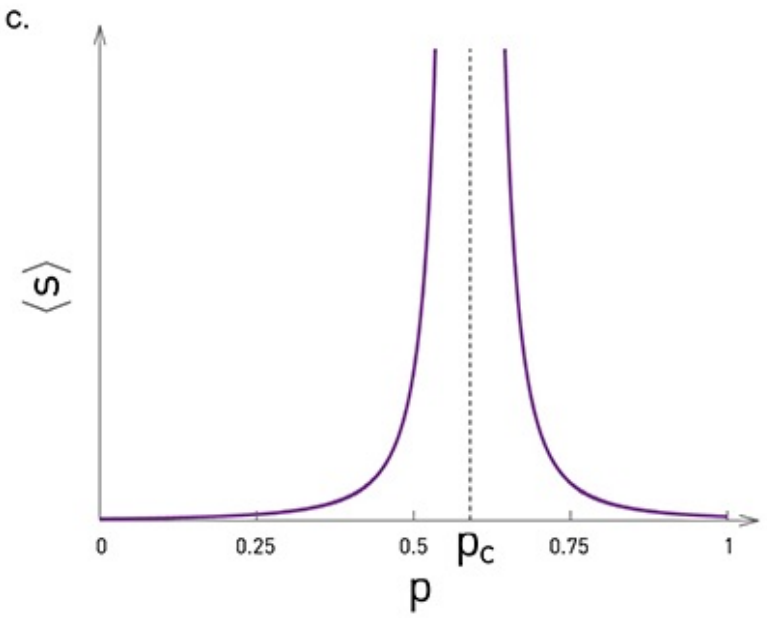
Order parameter

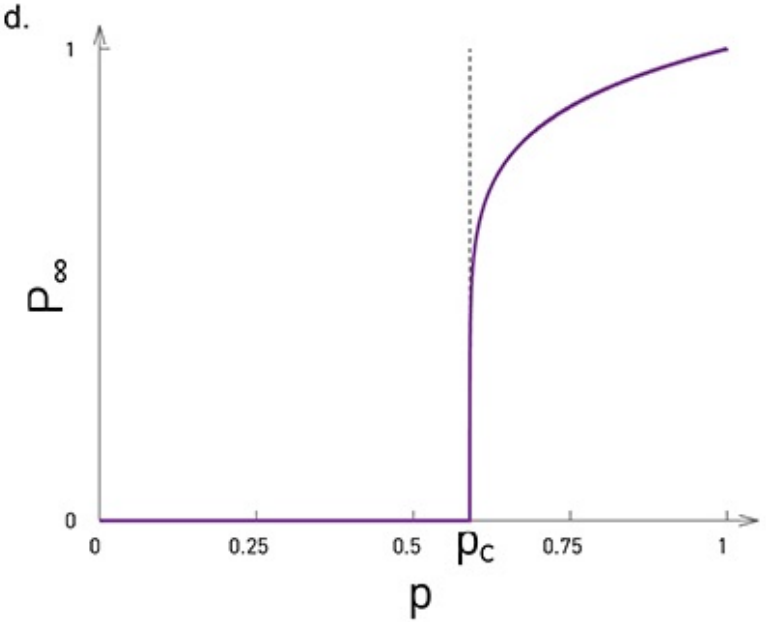
The probability that a randomly chosen node belongs to the largest cluster P_∞ defines the percolation state the system is in. If $P_\infty > 0$ there is a percolating cluster.

Correlation length and average cluster size

The mean distance between two nodes that belong to the same cluster ξ and the average cluster size $\langle S \rangle$ measure the typical size of connected nodes.

Percolation on 2D lattice





Percolation on 2D lattice

- **Average cluster size:** $\langle S \rangle \sim |p - p_c|^{-\gamma_p}$
- **Order Parameter:** $P_\infty \sim |p - p_c|^{\beta_p}$
- **Correlation Length:** $\xi \sim |p - p_c|^{-\nu_p}$

*The exponents γ_p, β_p, ν_p are called **critical exponents**, they characterise the system's behaviour near the critical point p_c*

- γ_p, β_p, ν_p are *universal*; they only depend on lattice **dimensionality**, not shape
- p_c depends on lattice **shape** (triangular, hexagonal, etc.)

Percolation on 2D lattice

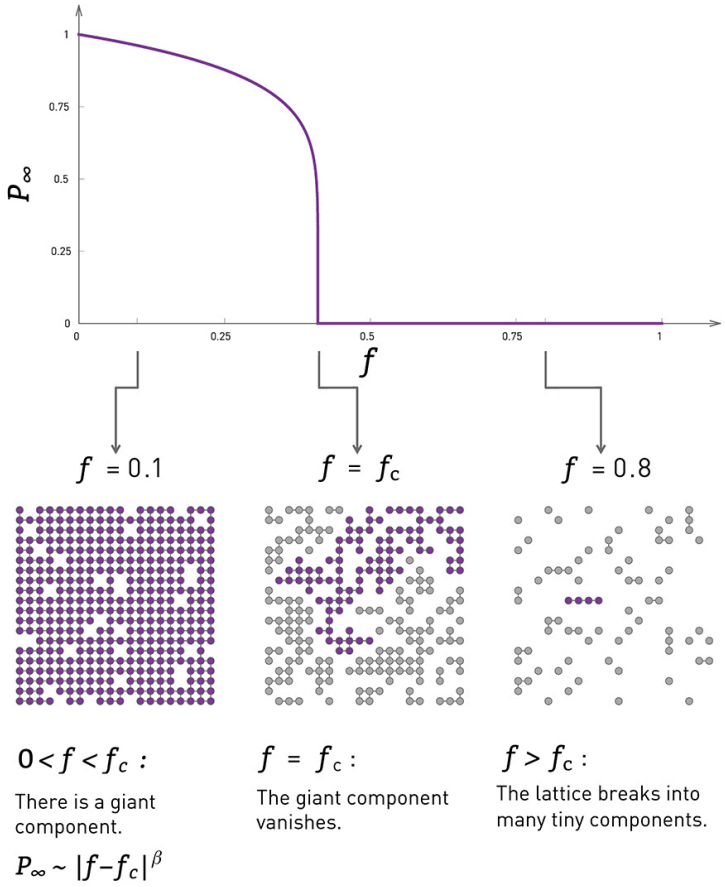
- **Average cluster size:** $\langle S \rangle \sim |p - p_c|^{-\gamma_p}$
- **Order Parameter:** $P_\infty \sim |p - p_c|^{\beta_p}$
- **Correlation Length:** $\xi \sim |p - p_c|^{-\nu_p}$

*The exponents γ_p, β_p, ν_p are called **critical exponents**, they characterise the system's behaviour near the critical point p_c*

- γ_p, β_p, ν_p are *universal*; they only depend on lattice **dimensionality**, not shape
- p_c depends on lattice **shape** (triangular, hexagonal, etc.)

Inverse Percolation and Robustness

Suppose we randomly remove fraction f of the nodes



Inverse percolation can be mapped into the problem of *percolation* by setting:

$$f = 1 - p$$

For lattices, once the fraction of removed nodes reaches critical value, the network breaks apart into many tiny components

Summary

- Breakdown of a network is **not a gradual process**
- Removing a small fraction of nodes has only limited impact on a network's integrity
- Once the fraction of removed nodes reaches a **critical threshold**, the network abruptly breaks into disconnected components
- Random node failures induce a **phase transition** from a connected to a fragmented network
- This transition in both regular and in random networks is characterised by percolation theory

Summary

- Breakdown of a network is **not a gradual process**
- Removing a small fraction of nodes has only limited impact on a network's integrity
- Once the fraction of removed nodes reaches a **critical threshold**, the network abruptly breaks into disconnected components
- Random node failures induce a **phase transition** from a connected to a fragmented network
- This transition in both regular and in random networks is characterised by percolation theory

Other forms of percolation

- **Site percolation:** It investigates the properties of the system when nodes are considered (for addition/removal)
- **Bond percolation:** It investigates the properties of the system when edges are considered (for addition/removal)
- **Directed percolation:** Each site can transmit its state to an unperturbed neighbour

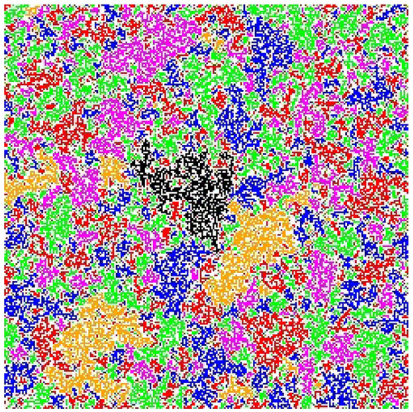
Explorables

https://www.complexity-explorables.org/explorables/baristas-secret/

Practical example: forest fire

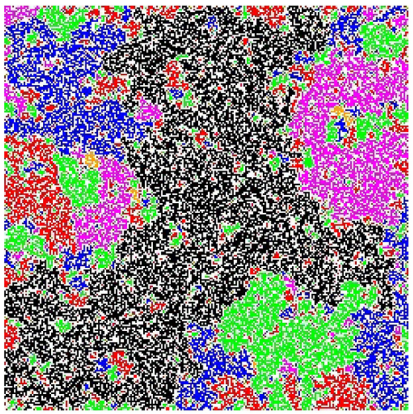
a.

p = 0 .55



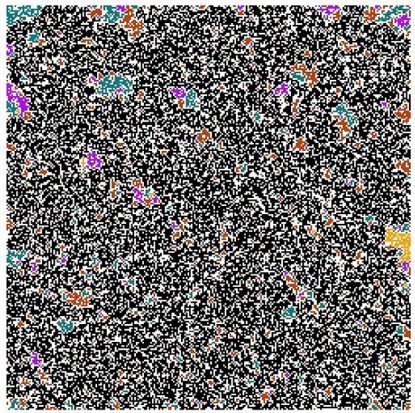
b.

p = 0 .593



c.

p = 0 .62



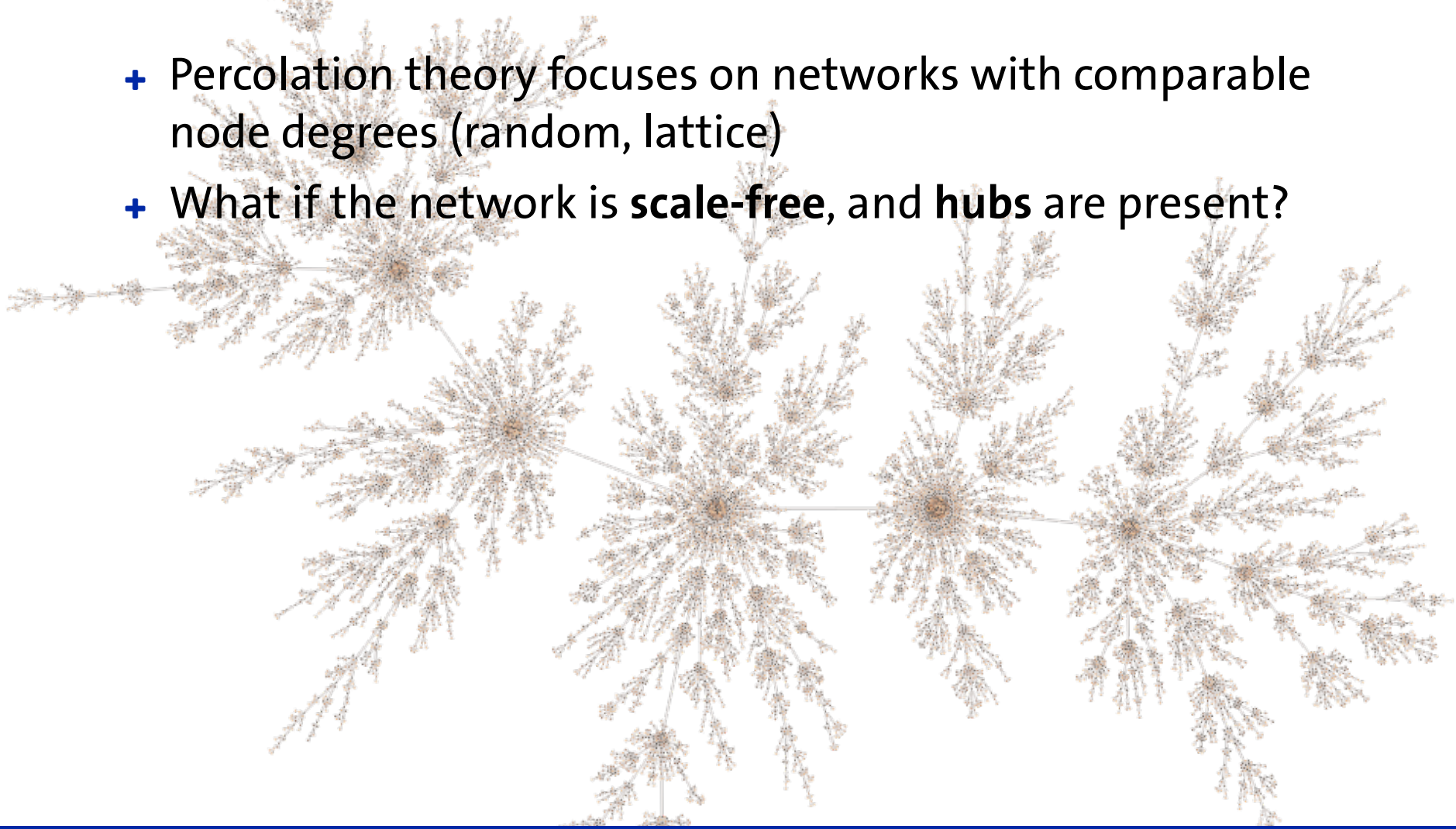
Explorables

https://www.complexity-explorables.org/explorables/critically-inflammatory/

Robustness of Scale-free Networks

Scale-free networks

- Percolation theory focuses on networks with comparable node degrees (random, lattice)
- What if the network is **scale-free**, and **hubs** are present?



Are scale-free networks more or less robust than homogeneous networks?

Experiment

1. We take a network (e.g. collected empirically)
2. At each time step, remove one node (site)
3. Compute the size of the largest connected component
4. Repeat 2-3 until all nodes have been

How to select which node to remove?

It can be

- at random
- based on some attack strategy (e.g. most connected or central remaining node)
- based on some node intrinsic (non-network related) property
- ...

Experiment

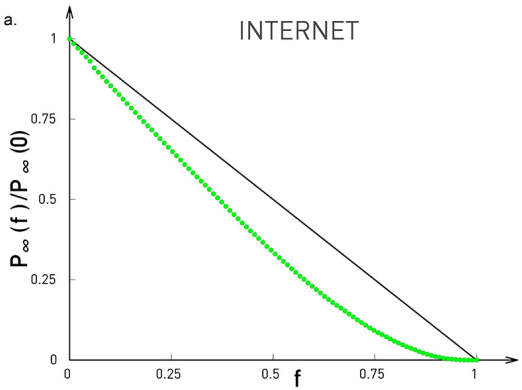
1. We take a network (e.g. collected empirically)
2. At each time step, remove one node (site)
3. Compute the size of the largest connected component
4. Repeat 2-3 until all nodes have been

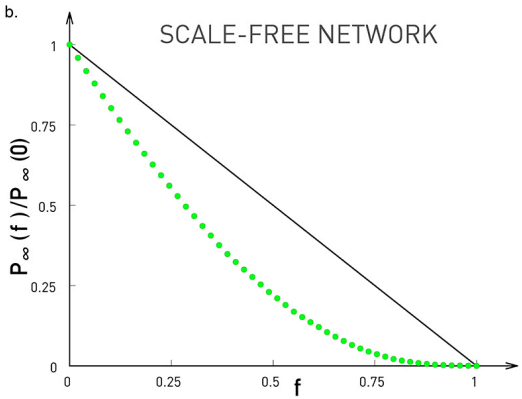
How to select which node to remove?

It can be

+ at random
+ based on some attack strategy (e.g. most connected or central remaining node)
+ based on some node intrinsic (non-network related) property
+ ...

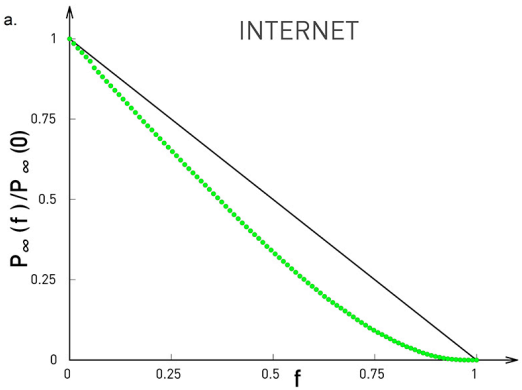
Robustness of Internet

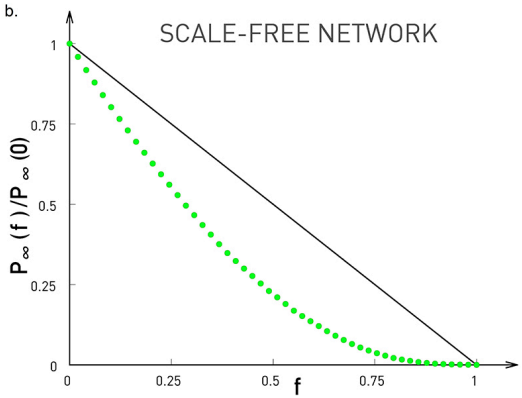




- (upper panel) Experiments on router-level network of internet (nodes: routers, links: physical connections)
- (lower panel) a synthetic scale-free network
- At each time-step one node is removed **at random** (multiple realisations are necessary)

Robustness of Internet



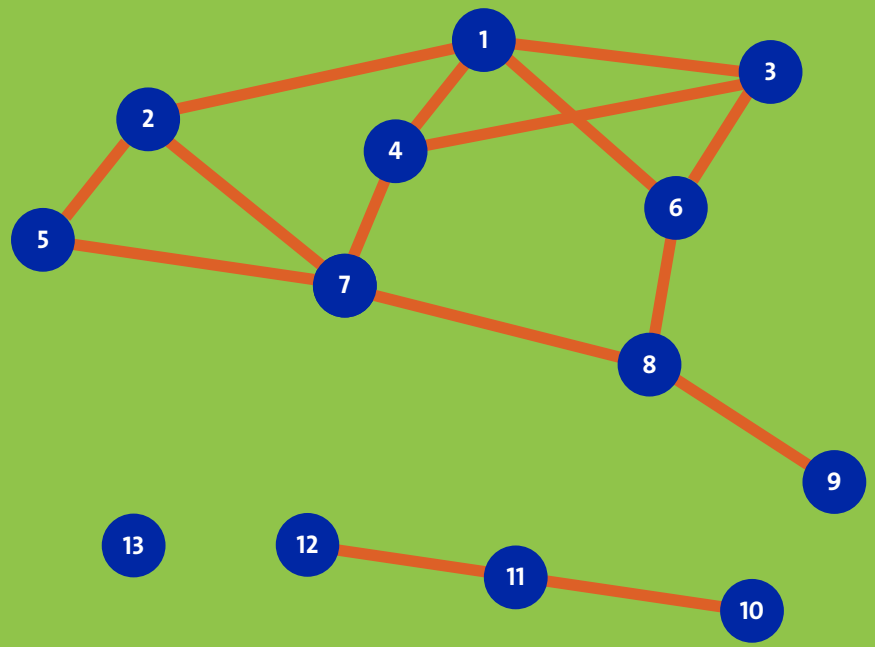


There is no critical point f_c above which the connected component breaks appart

*We should remove **all nodes** to destroy the connected component*

***Node** removal has always a limited impact on functionality*

Key observation



For a giant component to exist, on average each node in the component must have at least two links

Molloy-Reed Criterion

Molloy-Reed Criterion

A randomly wired network has a giant component if the following criterion holds.

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} > 2$$

Math details are on the supplementary document (authored by G. Bianconi)

Remember that $\langle\rangle$ denotes the average

Critical threshold

Critical threshold

One can derive a critical threshold for the fraction of nodes to be removed in order to break the giant component.

$$f_c = 1 - \frac{1}{\kappa - 1} \tag{1}$$

- f_c depends only on $\langle k^2 \rangle$, $\langle k \rangle$, which are **uniquely** defined by the degree distribution $P(k)$

Results for Erdős-Rényi networks

- The degree distribution can be approximated by a Poisson (cf. Session 5.1) when $\langle k \rangle \ll N$

$$P(k) = \exp\left(-\langle k \rangle\right) \frac{\langle k \rangle^k}{k!}$$

- It is simple to show that $\langle k^2 \rangle = \langle k \rangle (1 + \langle k \rangle)$

Results for Erdős-Rényi networks

- The degree distribution can be approximated by a Poisson (cf. Session 5.1) when $\langle k \rangle \ll N$

$$P(k) = \exp\left(-\langle k \rangle\right) \frac{\langle k \rangle^k}{k!}$$

- It is simple to show that $\langle k^2 \rangle = \langle k \rangle (1 + \langle k \rangle)$

Which implies

$$\kappa_{ER} = \frac{\langle k \rangle (1 + \langle k \rangle)}{\langle k \rangle} > 2 \iff \langle k \rangle > 1$$

Results for Erdős-Rényi networks

- The degree distribution can be approximated by a Poisson (cf. Session 5.1) when $\langle k \rangle \ll N$

$$P(k) = \exp\left(-\langle k \rangle\right) \frac{\langle k \rangle^k}{k!}$$

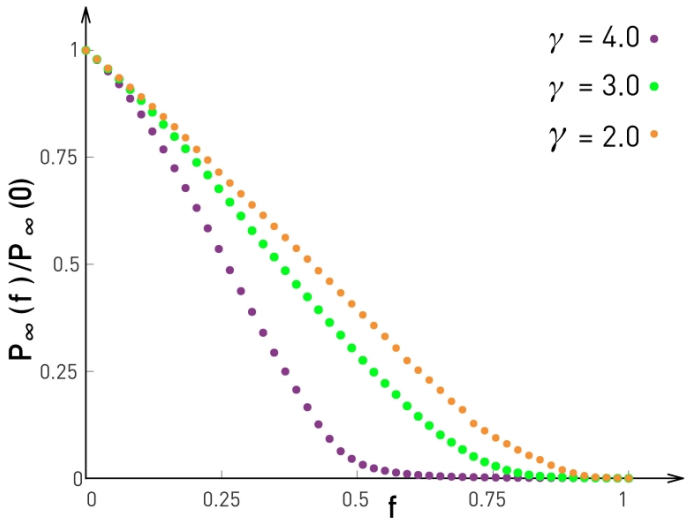
- It is simple to show that $\langle k^2 \rangle = \langle k \rangle (1 + \langle k \rangle)$

$$f_c^{ER} = 1 - \frac{1}{\langle k \rangle}$$

f_c^{ER} is always finite: ER network can always be broken apart with removal of finite fraction of nodes

Critical threshold for scale-free networks

- When $P(k) \propto k^{-\gamma}$, $\gamma < 3$, second moment $\langle k^2 \rangle \to \infty$ when $N \to \infty$
- Thus, $f_c \to 1$ for scale-free networks with a degree distribution with exponent $\gamma < 3$



Critical threshold for scale-free networks

It can be shown (see bibliography provided) that

$$f_c = \begin{cases} 1 - \frac{1}{\frac{\gamma-2}{3-\gamma} k_{min}^{\gamma-2} k_{max}^{3-\gamma} - 1}, & \text{if } 2 < \gamma < 3, \\ 1 - \frac{1}{\frac{\gamma-2}{\gamma-3} k_{min} - 1}, & \text{if } \gamma > 3 \end{cases}$$

- When $\gamma > 3$:
  - f_c depends only on γ and k_{min} and not on N
  - Scale-free network behaves like random network
  - It falls apart once a fraction of nodes $f_c \neq 1$ is removed
- When $\gamma < 3$:
  - f_c depends on γ, k_{min} and k_{max}
  - k_{max}, and thus, f_c depend on network size N
  - Therefore $f_c \to 1$ as $N \to \infty$
  - To fragment a SF network we must remove all of its nodes.

Critical threshold for scale-free networks

It can be shown (see bibliography provided) that

$$f_c = \begin{cases} 1 - \frac{1}{\frac{\gamma-2}{3-\gamma} k_{min}^{\gamma-2} k_{max}^{3-\gamma} - 1}, & \text{if } 2 < \gamma < 3, \\ 1 - \frac{1}{\frac{\gamma-2}{\gamma-3} k_{min} - 1}, & \text{if } \gamma > 3 \end{cases}$$

- When $\gamma > 3$:
  - f_c depends only on γ and k_{min} and not on N
  - Scale-free network behaves like random network
  - It falls apart once a fraction of nodes $f_c \neq 1$ is removed
- When $\gamma < 3$:
  - f_c depends on γ, k_{min} and k_{max}
  - k_{max}, and thus, f_c depend on network size N
  - Therefore $f_c \to 1$ as $N \to \infty$
  - To fragment a SF network we must remove all of its nodes.

Critical threshold for scale-free networks

It can be shown (see bibliography provided) that

$$f_c = \begin{cases} 1 - \frac{1}{\frac{\gamma-2}{3-\gamma} k_{min}^{\gamma-2} k_{max}^{3-\gamma} - 1}, & \text{if } 2 < \gamma < 3, \\ 1 - \frac{1}{\frac{\gamma-2}{\gamma-3} k_{min} - 1}, & \text{if } \gamma > 3 \end{cases}$$

- When $\gamma > 3$:
  - f_c depends only on γ and k_{min} and not on N
  - Scale-free network behaves like random network
  - It falls apart once a fraction of nodes $f_c \neq 1$ is removed
- When $\gamma < 3$:
  - f_c depends on γ, k_{min} and k_{max}
  - k_{max}, and thus, f_c depend on network size N
  - Therefore $f_c \to 1$ as $N \to \infty$
  - To fragment a SF network we must remove all of its nodes.

Robustness of scale-free networks

*Scale-free networks can withstand an **arbitrary level** of **random failures** without breaking apart*

- The hubs are responsible for this remarkable robustness
- There are far more small-degree nodes than hubs
- Therefore, random node removal will **most probably remove a small-degree node**, which is not critical

Robustness of scale-free networks

*Scale-free networks can withstand an **arbitrary level** of **random failures** without breaking apart*

- The hubs are responsible for this remarkable robustness
- There are far more small-degree nodes than hubs
- Therefore, random node removal will **most probably remove a small-degree node**, which is not critical

Robustness of Finite Networks

For finite networks, critical threshold can be approximated as:

$$f_c \approx 1 - \frac{C}{N^{\frac{3-\gamma}{\gamma-1}}} \tag{2}$$

- A network displays **enhanced robustness**, if $f_c > f_c^{ER}$
- Equivalently, when $\langle k^2 \rangle > \langle k \rangle (\langle k \rangle + 1)$
- This requirement is satisfied not only by scale-free networks
- Exponents γ_p, β_p, ν_p also change for scale-free networks

Robustness of Finite Networks

For finite networks, critical threshold can be approximated as:

$$f_c \approx 1 - \frac{C}{N^{\frac{3-\gamma}{\gamma-1}}} \tag{2}$$

- A network displays **enhanced robustness**, if $f_c > f_c^{ER}$
- Equivalently, when $\langle k^2 \rangle > \langle k \rangle (\langle k \rangle + 1)$
- This requirement is satisfied not only by scale-free networks
- Exponents γ_p, β_p, ν_p also change for scale-free networks

Breakdown Thresholds in Real Networks

Network	Random Failures (Real Network)	Random Failures (Randomized Network)	Attack (Real Network)
Internet	0.92	0.84	0.16
WWW	0.88	0.85	0.12
Power Grid	0.61	0.63	0.20
Mobile Phone Calls	0.78	0.68	0.20
Email	0.92	0.69	0.04
Science Collaboration	0.92	0.88	0.27
Actor Network	0.98	0.99	0.55
Citation Network	0.96	0.95	0.76
E. Coli Metabolism	0.96	0.90	0.49
Protein Interactions	0.88	0.66	0.06

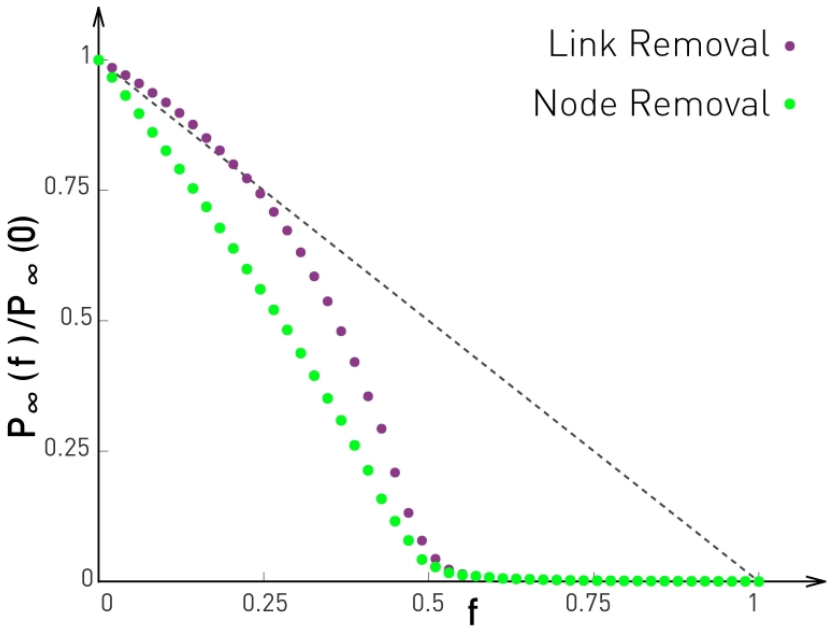
For most real networks, $f_c > f_c^{ER}$, indicating a larger robustness than if they were randomly architected

Robustness to link removal

What happens if we remove edges instead of nodes?

Link Removal

Theory predicts $f_c^{node} = f_c^{link}$



E.g. this random network with $\langle k \rangle = 2$ falls apart at $f_c = 0.5$

Summary

For random removal

- Breakdown threshold f_c **only** depends on $\langle k^2 \rangle$ and $\langle k \rangle$
- They are **uniquely** determined by the **degree distribution**
- For scale-free networks with $\gamma < 3, f_c \to 1$
- This means that we need too remove **all nodes** to break a scale-free network
- Robust are all networks, for which $\langle k^2 \rangle > \langle k \rangle (\langle k \rangle + 1)$

Summary

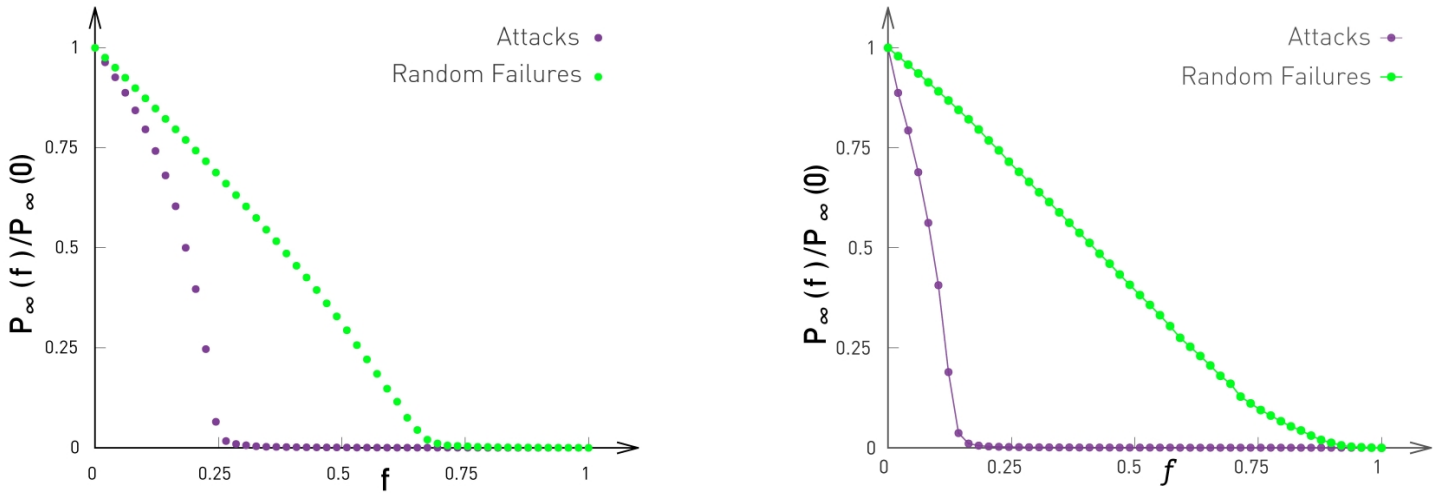
For random removal

- Breakdown threshold f_c **only** depends on $\langle k^2 \rangle$ and $\langle k \rangle$
- They are **uniquely** determined by the **degree distribution**
- For scale-free networks with $\gamma < 3, f_c \to 1$
- This means that we need too remove **all nodes** to break a scale-free network
- Robust are all networks, for which $\langle k^2 \rangle > \langle k \rangle (\langle k \rangle + 1)$

Robustness to targeted attacks

What happens if the node selection targets the remaining most connected node?

Results for targeted attacks



Results for targeted attacks: (left panel) ER Network, (right panel) BA network

Scale-free networks are more fragile to targetted attacks and their functioning deteriorates more rapidly than random networks!

Key points

- Real networks are **robust** to random node failures
- Robustness originates from the fact that random failures **mostly affect numerous small nodes**, which are not critical
- At the same time, they are more fragile to targeted attacks

Cascading Failures

Cascading Failures

- Before: we assumed that each node failure was independent from others.
- Reality: the activity of each node **depends** on the activity of its **neighbouring** nodes.

Consequently the failure of a node can induce the failure of the nodes connected to it.

Cascading Failures: examples

- **Power grid**: failure of one node causes electric currents to be reorganised to other nodes, increasing load
- **Internet**: if a router fails to transmit the packages, Internet protocols recommend neighbouring routers to look for alternative routes, increasing traffic on other routers
- **Finance**: Drop in house prices induced cascade of failed banks and companies

Cascading Failures: examples

- **Power grid**: failure of one node causes electric currents to be reorganised to other nodes, increasing load
- **Internet**: if a router fails to transmit the packages, Internet protocols recommend neighbouring routers to look for alternative routes, increasing traffic on other routers
- **Finance**: Drop in house prices induced cascade of failed banks and companies

Cascading Failures: examples

- **Power grid**: failure of one node causes electric currents to be reorganised to other nodes, increasing load
- **Internet**: if a router fails to transmit the packages, Internet protocols recommend neighbouring routers to look for alternative routes, increasing traffic on other routers
- **Finance**: Drop in house prices induced cascade of failed banks and companies

Cascading Failures: features

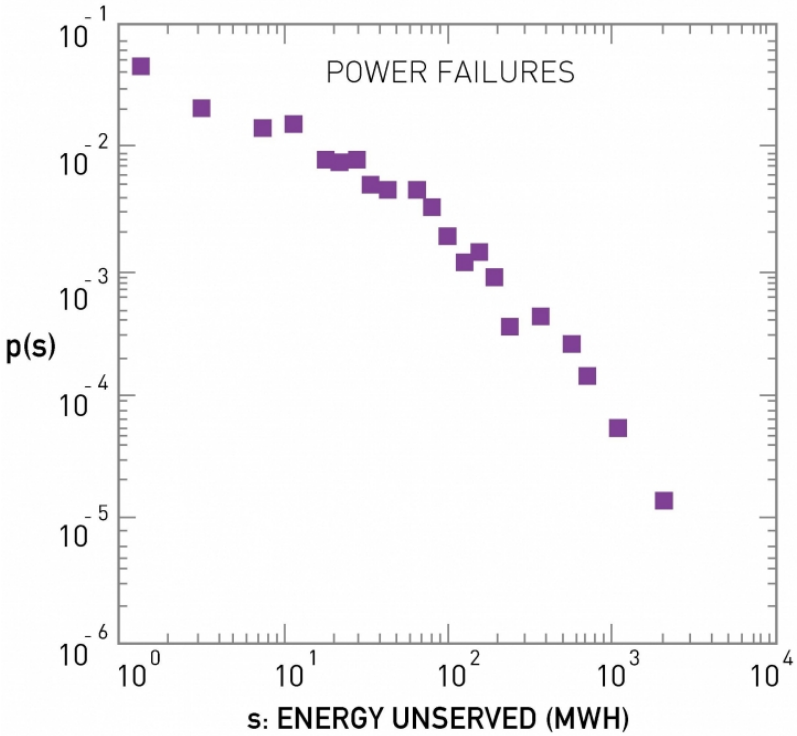
- Initial failure had only **limited impact** on the whole network
- Initial failure did **not** stay **localised**
- It **spread** along the links of the network, inducing additional failures.
- Eventually, multiple nodes lost their ability to carry out their normal functions.
- Each of these systems experienced **cascading failures**

Cascading Failures: features

- Initial failure had only **limited impact** on the whole network
- Initial failure did **not** stay **localised**
- It **spread** along the links of the network, inducing additional failures.
- Eventually, multiple nodes lost their ability to carry out their normal functions.
- Each of these systems experienced **cascading failures**

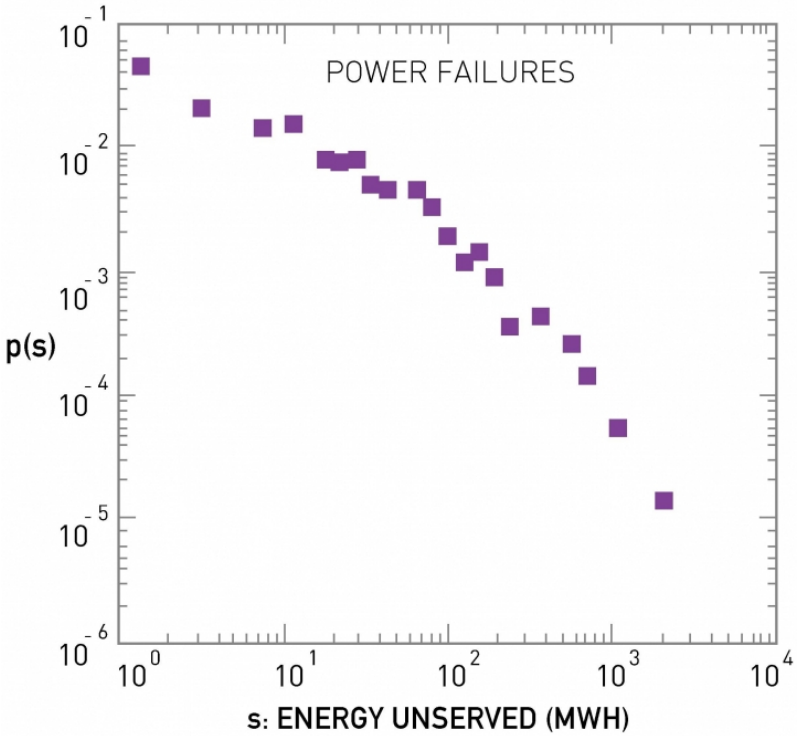
Examples of cascading failures: Blackouts

- Can be caused by power station failure, damage to transmission lines, short circuit, etc
- Such failure **redistributes** the power from the failed component to other components
- A frequently recorded measure of blackout size is the energy unserved:
  $P(s) \sim s^{-\alpha}$, where α is the *avalanche exponent*
- **Power-law** nature indicates that most blackouts are rather small



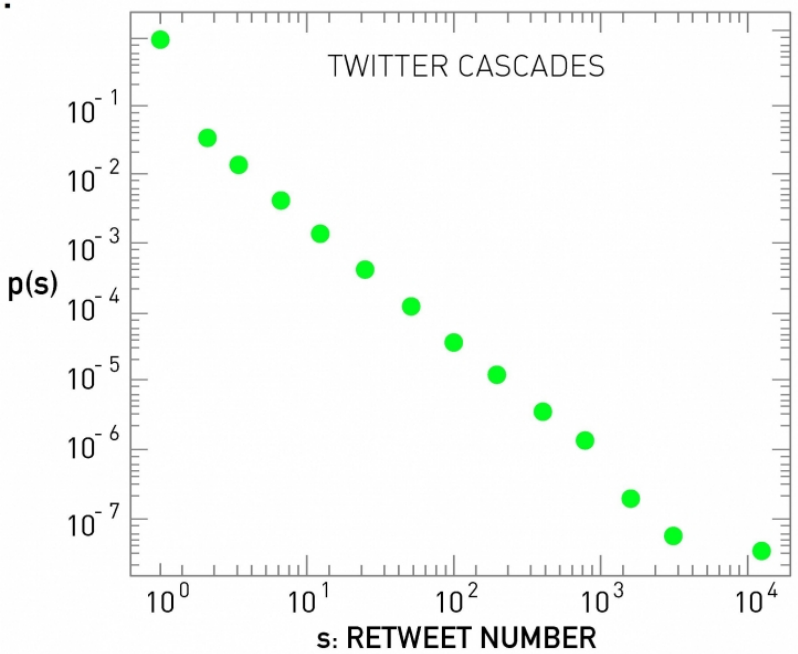
Examples of cascading failures: Blackouts

- Can be caused by power station failure, damage to transmission lines, short circuit, etc
- Such failure **redistributes** the power from the failed component to other components
- A frequently recorded measure of blackout size is the energy unserved:
  $P(s) \sim s^{-\alpha}$, where α is the *avalanche exponent*
- **Power-law** nature indicates that most blackouts are rather small



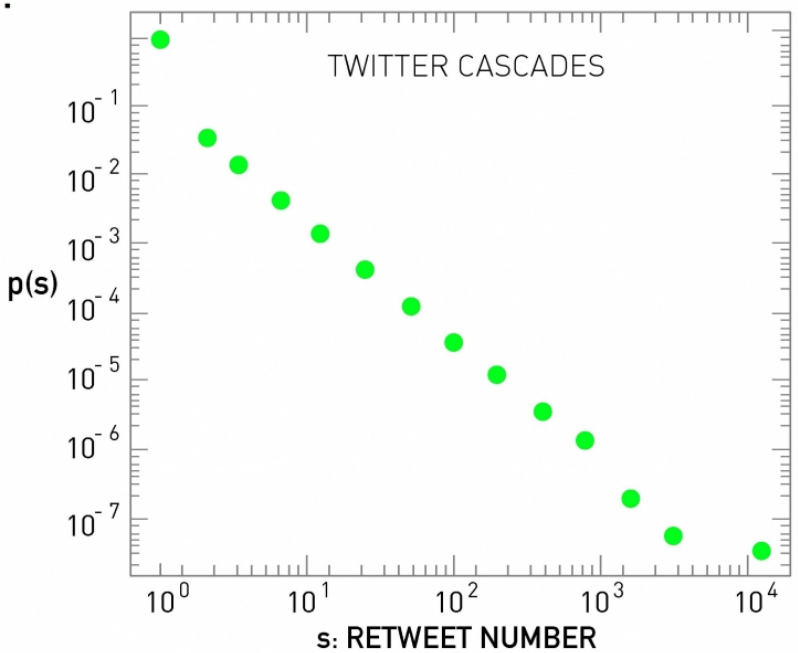
Examples of cascading failures: Information

- The micro-blogging service Twitter has been particularly studied in this context
- Study: track 74 million reposts over 2 months
- These cascades also follow **power-law** distribution with $\alpha = 1.75$
- Average cascade size is only $\langle s \rangle = 1.14$



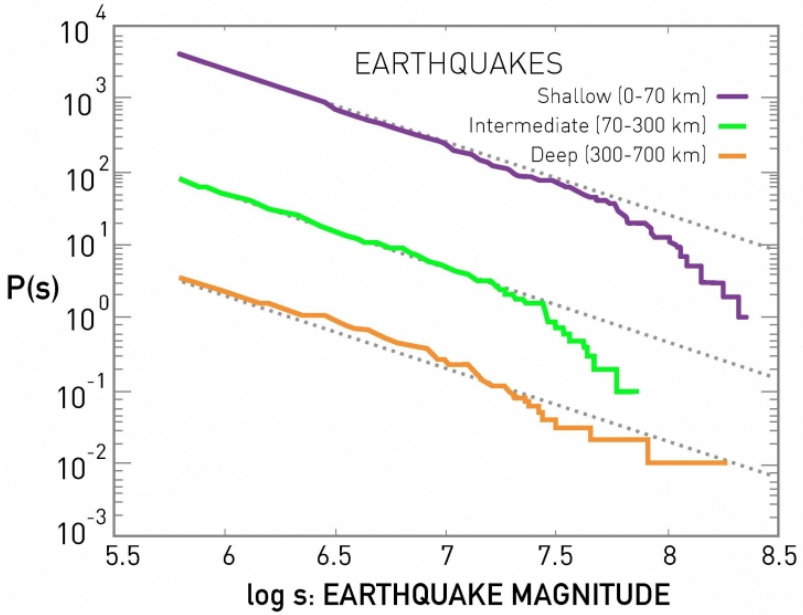
Examples of cascading failures: Information

- The micro-blogging service Twitter has been particularly studied in this context
- Study: track 74 million reposts over 2 months
- These cascades also follow **power-law** distribution with $\alpha = 1.75$
- Average cascade size is only $\langle s \rangle = 1.14$



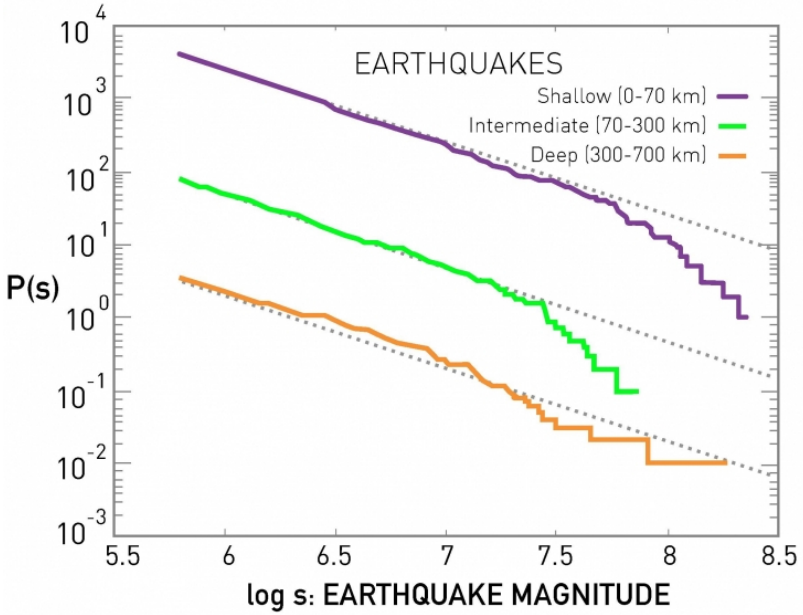
Examples of cascading failures: Earthquakes

- Once a fault has locked, the continued relative motion of the tectonic plates **accumulates** strain energy.
- When the stress becomes sufficient, a sudden slide releases the stored energy, causing an earthquake.
- Distribution of earthquake amplitudes is a **power-law** with $\alpha = 1.67$



Examples of cascading failures: Earthquakes

- Once a fault has locked, the continued relative motion of the tectonic plates **accumulates** strain energy.
- When the stress becomes sufficient, a sudden slide releases the stored energy, causing an earthquake.
- Distribution of earthquake amplitudes is a **power-law** with $\alpha = 1.67$



Cascading failures in other fields

- Bad weather or mechanical failures can cascade through *airline schedules*, delaying multiple flights
- Disappearance of single species can cascade through the *food web of an ecosystem*, inducing the extinction of numerous species
- The shortage of a particular component can cripple supply chains;
  Example: the 2011 floods in Thailand have resulted in a chronic shortage of car components all over the world, which resulted in worldwide insurance claims reaching $20 billion.

Avalanche Exponents in Real Systems

Source	Exponent	Cascade
Power grid (North America)	2.0	Power
Power grid (Sweden)	1.6	Energy
Power grid (Norway)	1.7	Power
Power grid (New Zealand)	1.6	Energy
Power grid (China)	1.8	Energy
Twitter Cascades	1.75	Retweets
Earthquakes	1.67	Seismic Wave

Avalanche exponents are surprisingly close to each other

Summary

- **Cascading** effects are observed in systems of rather **different nature**
- Distribution of cascade sizes is a **power-law**
- Thus, **most** cascades are **too small** to be noticed
- But there are a **few** huge ones, having a **global** impact
  - 2003 power outage in North America
  - the tweet Iran Election Crisis: 10 Incredible YouTube Videos http://bit.ly/vPDLo that was shared 1,399 times
  - January 2010 earthquake in Haiti, with over 200,000 victims

Modeling Cascading Failures

Cascading systems

- Cascading events depend on many factors (network structure, breakdown criteria for each node, etc)
- Despite diversity of these factors, distribution of cascade sizes is universal
- Cascades always follow power-law nature. Why?
- Systems that develop cascades share three key ingredients:
  1. System is characterised by some **flow** over a network (electric current, information, etc)
  2. Each component has a local **breakdown** rule
  3. System has a mechanism to **redistribute** the flow to other nodes upon a failure

Cascading systems

- Cascading events depend on many factors (network structure, breakdown criteria for each node, etc)
- Despite diversity of these factors, distribution of cascade sizes is universal
- Cascades always follow power-law nature. Why?
- Systems that develop cascades share three key ingredients:
  1. System is characterised by some **flow** over a network (electric current, information, etc)
  2. Each component has a local **breakdown** rule
  3. System has a mechanism to **redistribute** the flow to other nodes upon a failure

Failure propagation model: setting

- Consider a network with arbitrary degree distribution
- Each **node** i can be in **state** $s_i = 0$ (active or healthy) and $s_i = 1$ (inactive or failed)
- Each node is characterised by a breakdown **threshold** $\phi_i = \phi \forall i$

Failure propagation model: propagation

1. Initially all nodes are healthy $s_i = 0$ for all i
2. At time $t = 0$ one node j switches to $s_j \to 1$ (initial failure)
3. At all times $t = 1, 2...$:
   - 3.1 Randomly pick a node n
   - 3.2 If $s_n = 1$, do nothing
   - 3.3 If $s_n = 0$:
     - Inspect state of k_n of neighbours of the chosen node
     - If fraction of failed neighbours is at least ϕ, change the state $s_n \to 1$, otherwise, leave $s_n = 0$

Failure propagation model: regimes

[1.] Subcritical regime:

- $\langle k \rangle$ is high, change of state is unlikely, as healthy nodes have many healthy neighbours;
- Cascades die out quickly
- Cascade sizes follow exponential distribution
- The system is unable to support large global cascades

Failure propagation model: regimes

[2.] Supercritical regime:

- $\langle k \rangle$ is small
- Change of state of a single node triggers several its neighbours to change state too
- Global cascades occur
- Perturbations induce major breakdowns

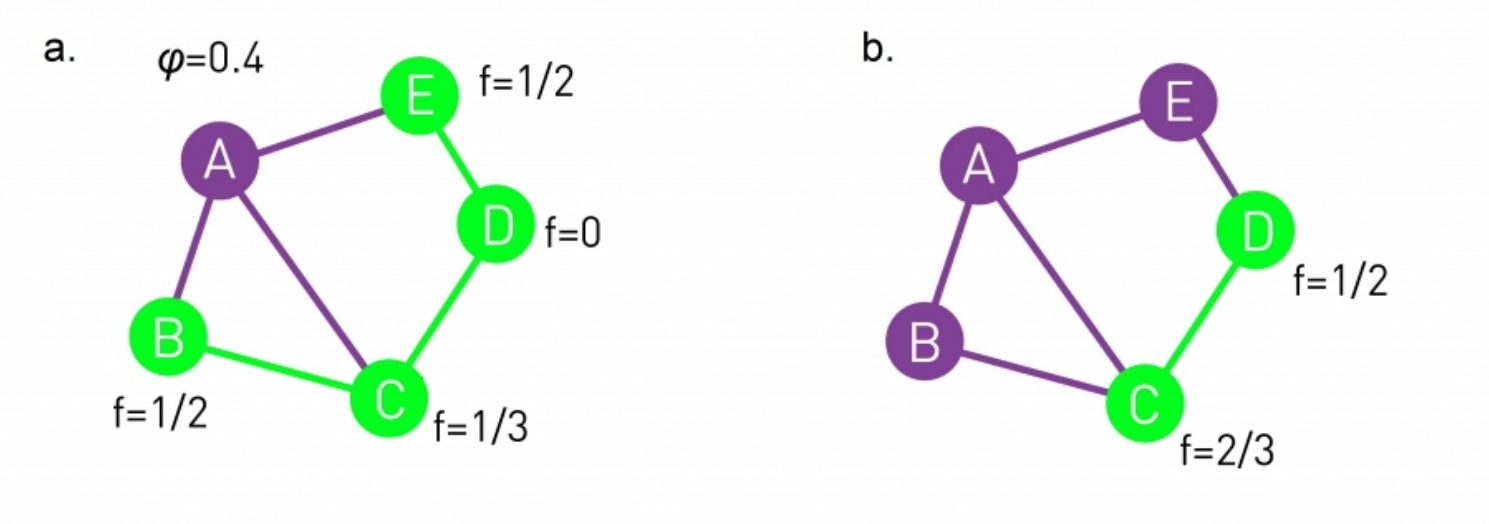
Failure propagation model: regimes

[3.] Critical regime:

- At the boundary
- The avalanches have widely different sizes
- Cascade sizes s follow power-law distribution

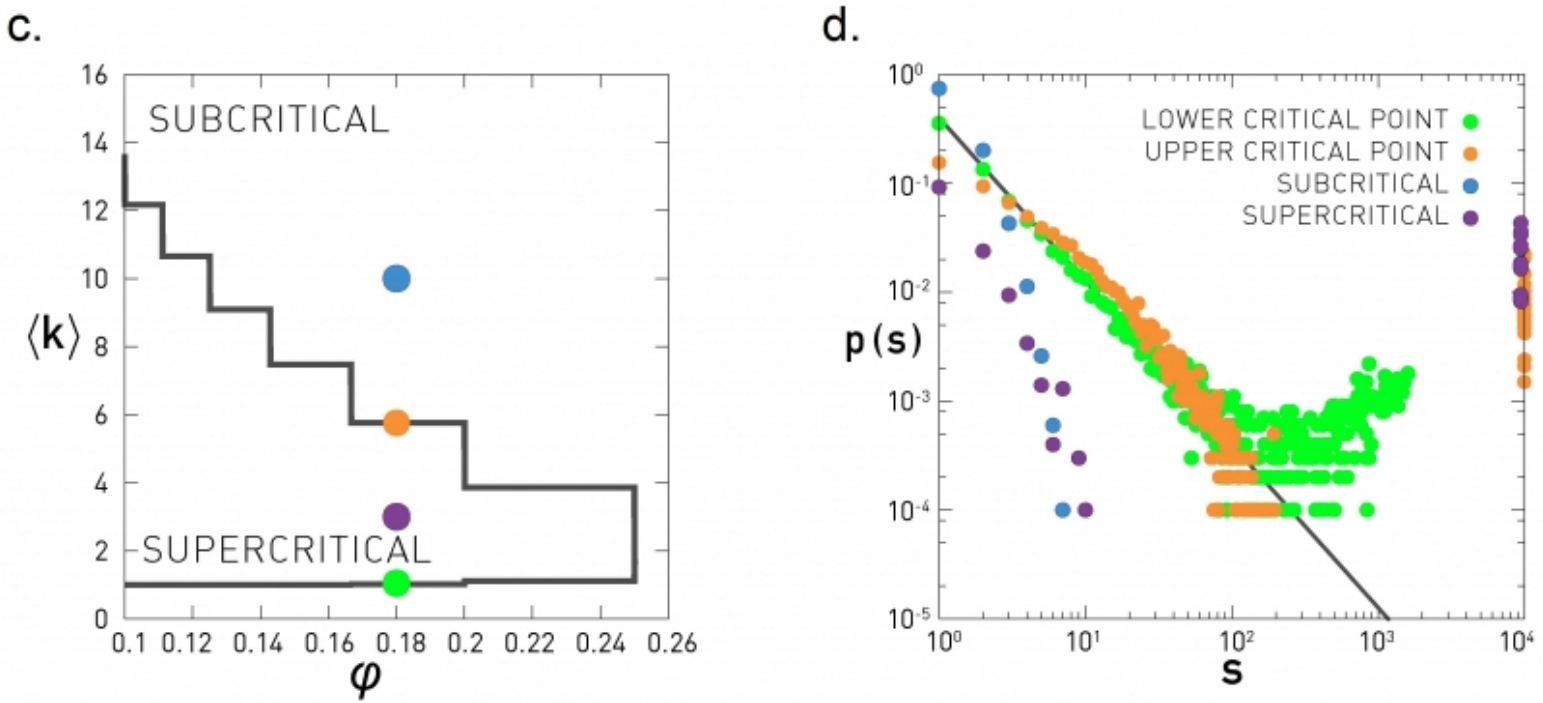
$$P(s) \sim s^{-\alpha} \qquad \alpha^{ER} = 1.5$$

Failure propagation model: simulation



- All nodes have threshold $\phi = 0.4$
- Cascade starts with node A
- After 2 steps, cascade takes over the whole network

Failure propagation model: regimes



Branching model

Branching model

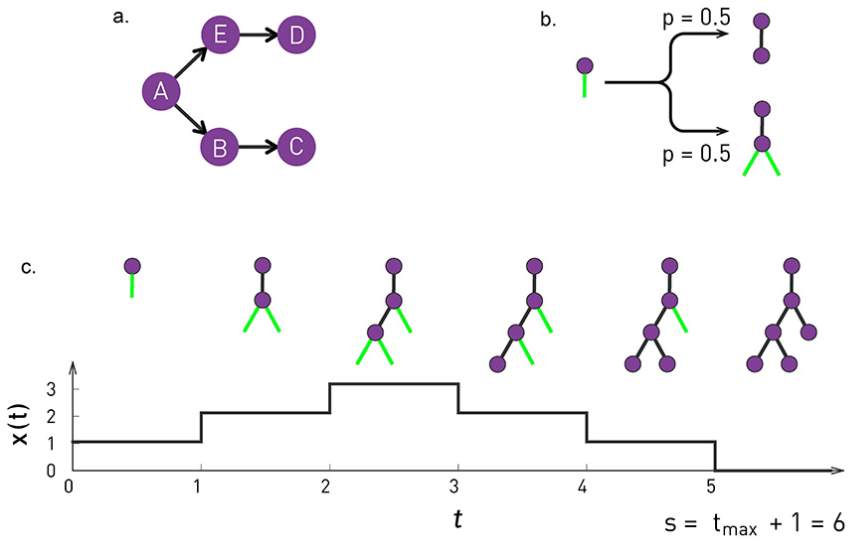
- Failure propagation model is too complex for predictions
- Branching model helps to understand the power-law and calculate α
- **Observation**: each cascading failure follows a branching process

Branching model: setting

- The node whose initial failure triggers the avalanche is the **root of the tree**
- The branches of the tree are the nodes whose failure was triggered by this initial failure

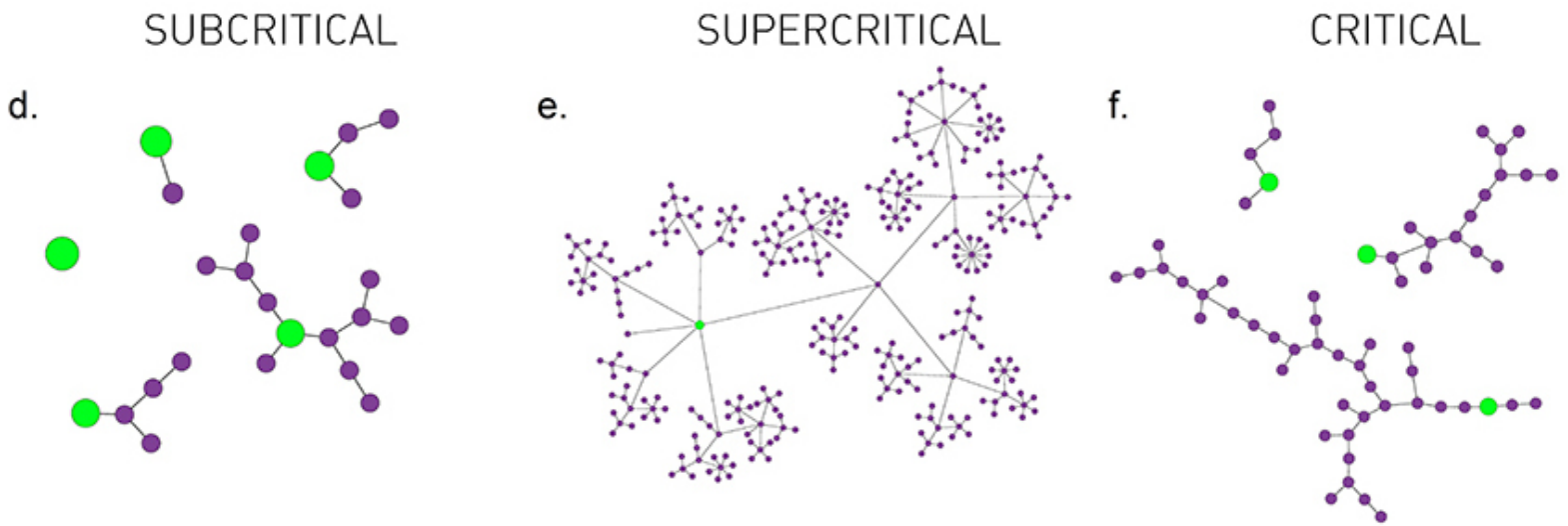
Branching model: propagation

1. The model starts with a single active node (root) at $t = 0$
2. At $t = 1, 2, \ldots$:
   - **2.1** Each active node produces k offsprings, drawn from $P(k)$
   - **2.2** If $k = 0$, the branch dies out
   - **2.3** If $k > 0$, there are k new active nodes



Branching model: regimes

- Subcritical
- Supercritical
- Critical



Branching model: regimes

1. Subcritical regime:
   - $\langle k \rangle < 1$
   - Each branch has less than 1 offspring
   - Avalanche size follow exponential distribution
2. Supercritical regime:
   - $\langle k \rangle > 1$
   - Each branch has more than 1 offspring
   - All avalanches are global, tree grows indefinitely
3. Critical regime:
   - $\langle k \rangle = 1$
   - Each branch has exactly 1 offspring
   - Avalanche size follow power-law distribution

Branching model: regimes

1. Subcritical regime:
   - $\langle k \rangle < 1$
   - Each branch has less than 1 offspring
   - Avalanche size follow exponential distribution
2. Supercritical regime:
   - $\langle k \rangle > 1$
   - Each branch has more than 1 offspring
   - All avalanches are global, tree grows indefinitely
3. Critical regime:
   - $\langle k \rangle = 1$
   - Each branch has exactly 1 offspring
   - Avalanche size follow power-law distribution

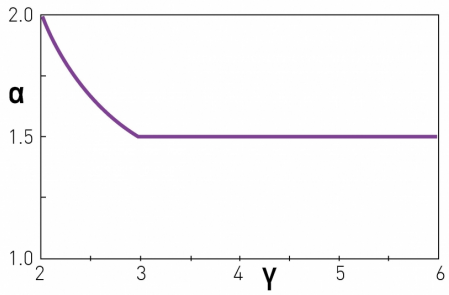
Branching model: regimes

1. Subcritical regime:
   - $\langle k \rangle < 1$
   - Each branch has less than 1 offspring
   - Avalanche size follow exponential distribution
2. Supercritical regime:
   - $\langle k \rangle > 1$
   - Each branch has more than 1 offspring
   - All avalanches are global, tree grows indefinitely
3. Critical regime:
   - $\langle k \rangle = 1$
   - Each branch has exactly 1 offspring
   - Avalanche size follow power-law distribution

Branching model: avalanche size distribution

- Branching model can be solved **analytically**
- We can determine avalanche size distribution for any $P(k)$
- If $P(k)$ has exponential tail, $\alpha = 1.5$
- If $P(k)$ is scale-free, avalanche exponent depends on the power-law exponent as

$$\alpha = \begin{cases} 1.5, \text{ if } \gamma \geq 3, \\ \frac{\gamma}{\gamma - 1}, \text{ if } 2 < \gamma < 3 \end{cases}$$



Explorables

https://www.complexity-explorables.org/explorables/the-blob/

Summary

- Two models for simulation of cascading failures: **failure propagation** and **branching model**
- There exist other models: overload, sand pile, etc
- The models differ in their realism and number of parameters
- **All models** predict the existing of **critical regime**, when avalanche sizes follow power-law distribution
- Avalanche exponent α is **uniquely** determined by node degree distribution $P(k)$

Summary

- Two models for simulation of cascading failures: **failure propagation** and **branching model**
- There exist other models: overload, sand pile, etc
- The models differ in their realism and number of parameters
- **All models** predict the existing of **critical regime**, when avalanche sizes follow power-law distribution
- Avalanche exponent α is **uniquely** determined by node degree distribution $P(k)$

Summary

- Two models for simulation of cascading failures: **failure propagation** and **branching model**
- There exist other models: overload, sand pile, etc
- The models differ in their realism and number of parameters
- **All models** predict the existing of **critical regime**, when avalanche sizes follow power-law distribution
- Avalanche exponent α is **uniquely** determined by node degree distribution $P(k)$

References I

- Albert-Laszlo Barbasi, *Network Science*, Cambridge University Press, 2015

Universität Zürich[UZH]

Blockchain & Distributed Ledger Technologies

UZH Blockchain Center

Claudio J. Tessone

Blockchain & Distributed Ledger Technologies
UZH Blockchain Center

claudio.tessone@uzh.ch
http://www.ifi.uzh.ch/bdlt