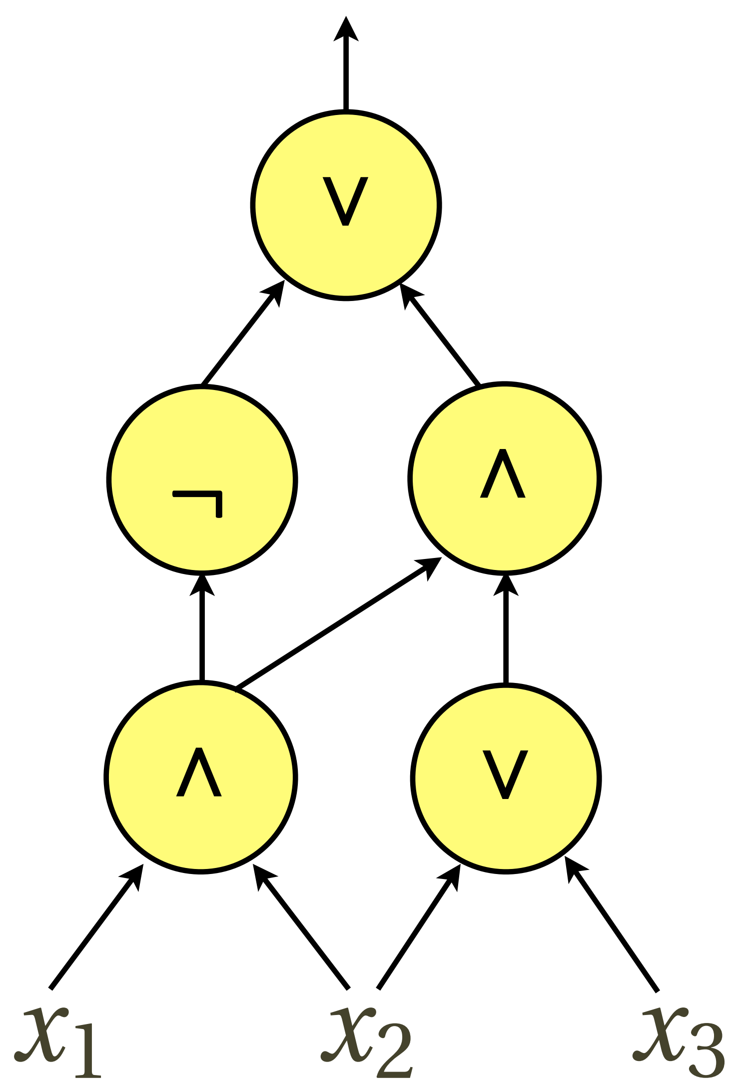
Combinatorics

南京大学
尹一通

Circuit Complexity

Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$

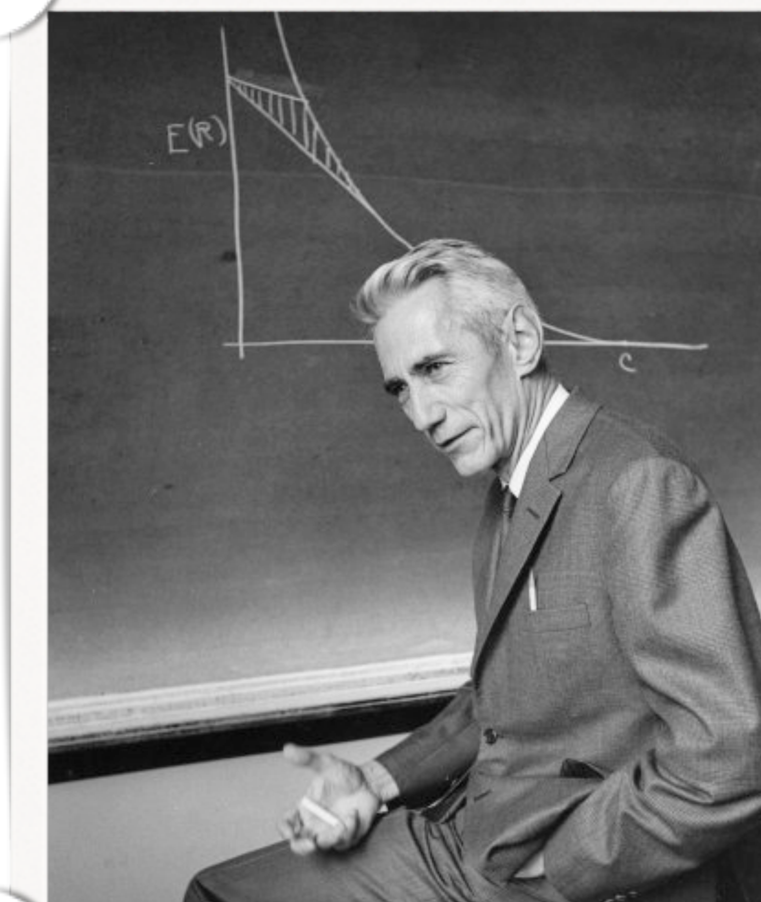
Boolean circuit



- DAG (directed acyclic graph)
- Nodes:
  - inputs: $x_1 \ldots x_n$
  - gates: ∧ ∨ ¬
- Complexity: #gates

Theorem (Shannon 1949)

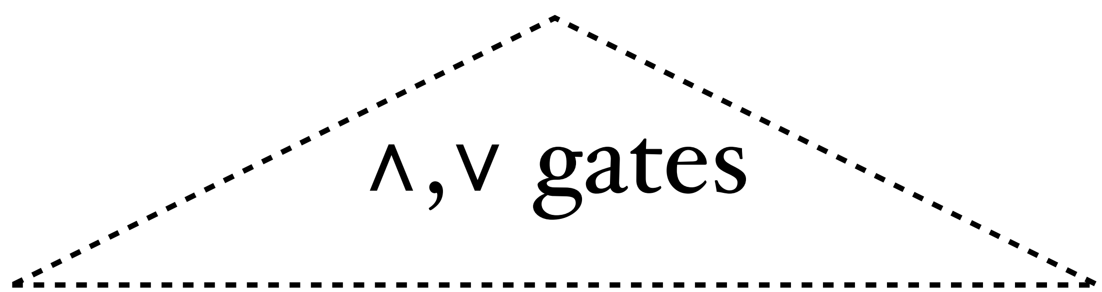
There is a boolean function $f : \{0,1\}^n \to \{0,1\}$ which cannot be computed by any circuit with $\frac{2^n}{3n}$ gates.



Claude Shannon

of $f : \{0,1\}^n \to \{0,1\}$ $\qquad \left| \{0,1\}^{2^n} \right| = 2^{2^n}$

of circuits with *t* gates: $\quad < \quad 2^t (2n + t + 1)^{2t}$

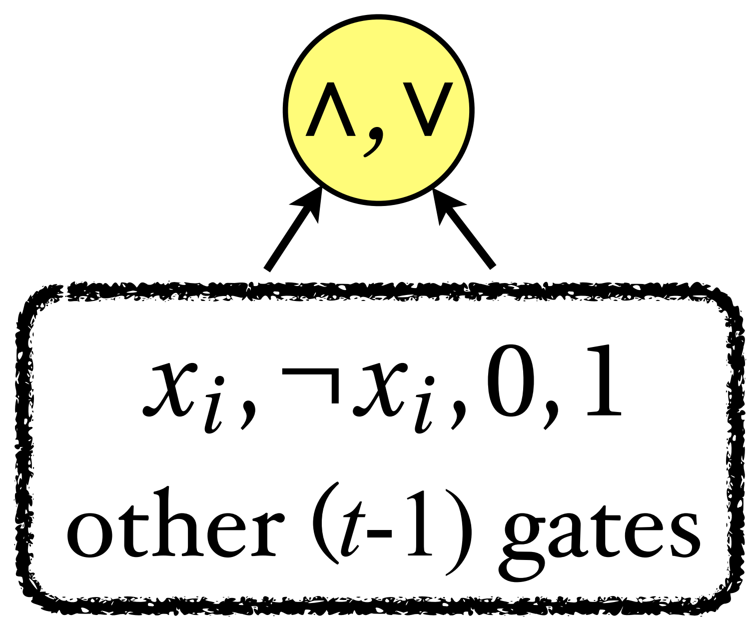


$x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n, 0, 1$

De Morgan's law:

$$\neg(A \vee B) = \neg A \wedge \neg B$$

$$\neg(A \wedge B) = \neg A \vee \neg B$$



Theorem (Shannon 1949)

Almost all

~~There is a~~ boolean function $f : \{0,1\}^n \to \{0,1\}$ which cannot be computed by any circuit with $\frac{2^n}{3n}$ gates.

one circuit computes one function

$\#f$ computable by t gates ≤

#circuits with t gates ≤

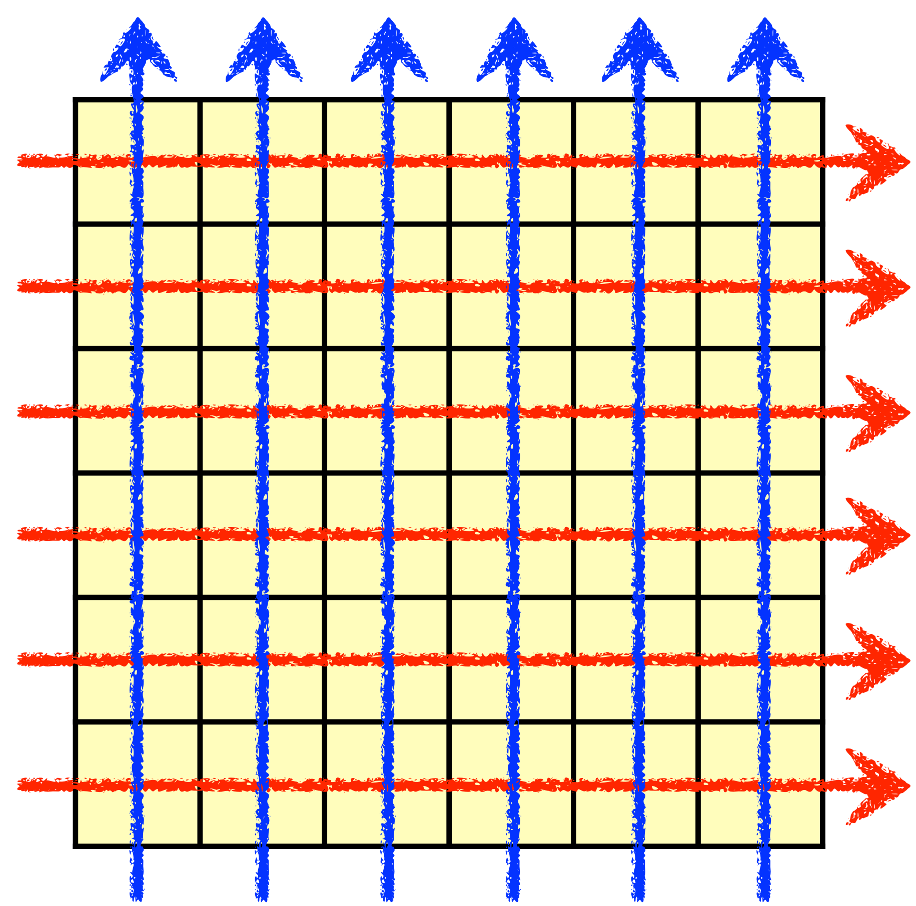
$$2^t(2n+t+1)^{2t} \ll 2^{2^n} = \#f$$

$$t = 2^n/3n$$

Double Counting

"Count the same thing twice. The result will be the same."

sum by row
A



A=B

sum by column
B

Handshaking lemma

A party of *n* guests.

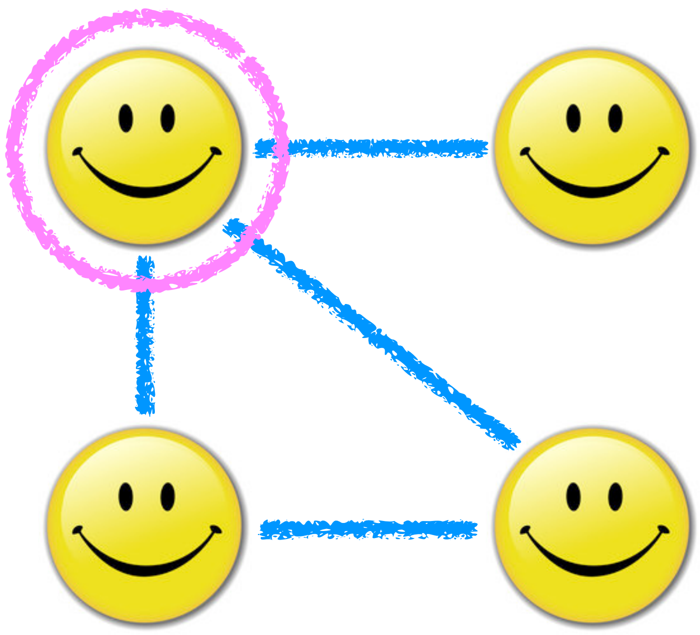
> The number of guests who shake hands an odd number of times is even.

Modeling:

n guests ⇔ *n* vertices

handshaking ⇔ edge

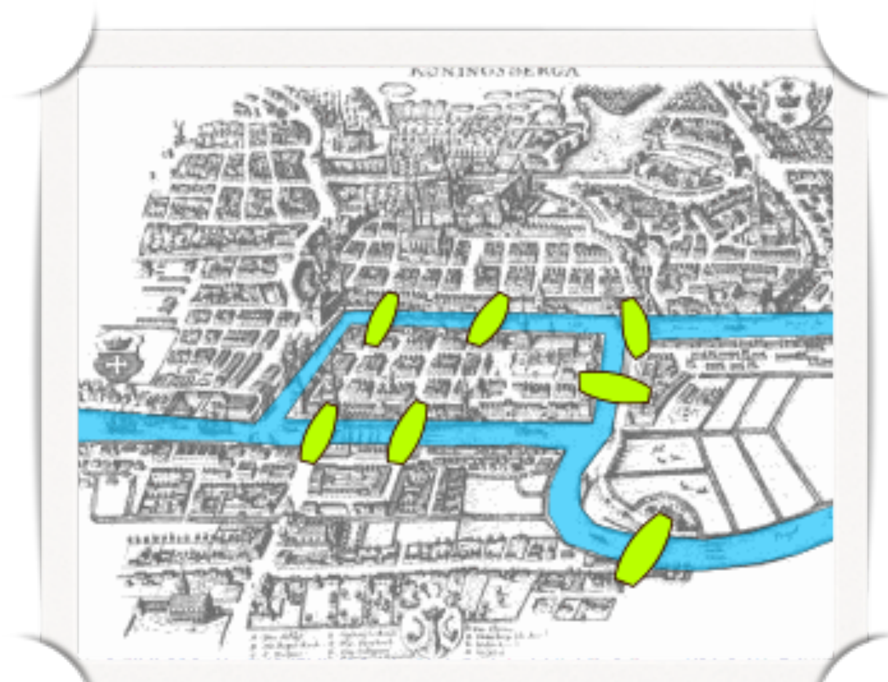
# of handshaking ⇔ degree



Lemma (Euler 1736)

$$\sum_{v \in V} d(v) = 2|E|$$

Leonhard Euler



In the 1736 paper of Seven Bridges of Königsberg

Lemma (Euler 1736)

$$\sum_{v \in V} d(v) = 2|E|$$

Count directed edges:

$$(u, v) : \{u, v\} \in E$$

Count by vertex:

$\forall v \in V$

d directed edges

$(v, u_1) \cdots (v, u_d)$

=

Count by edge:

$\forall \{u, v\} \in E$

2 directions

(u, v) and (v, u)

Lemma (Euler 1736)

$$\sum_{v \in V} d(v) = 2|E|$$

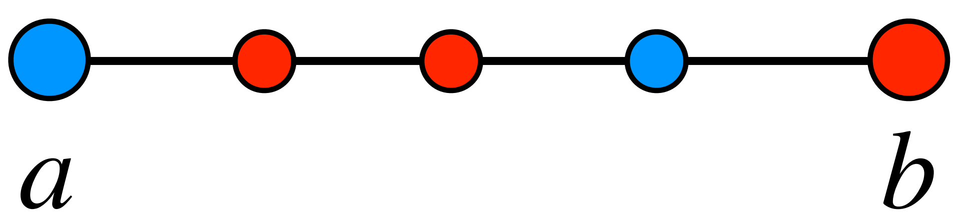
Corollary

# of odd-degree vertices is even.

Sperner's Lemma

line segment: *ab* divided into small segments

each endpoint: red or blue

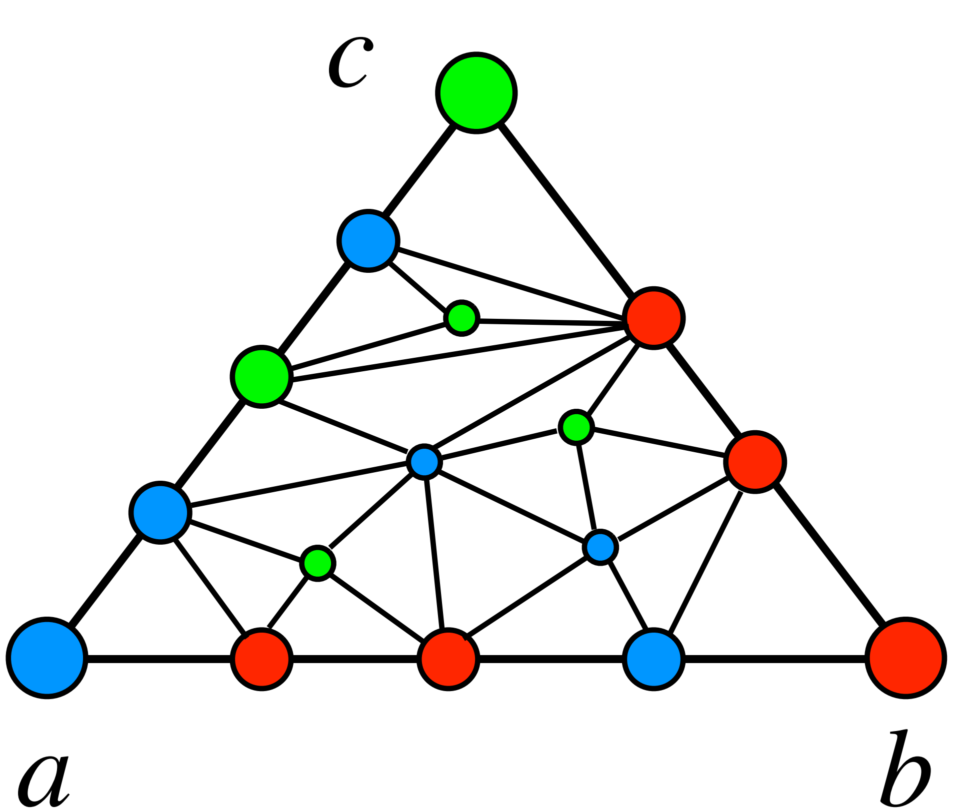


ab have different color

∃ small segment 

Emanuel Sperner

Sperner's Lemma



triangle: abc

triangulation

proper coloring:

3 colors red, blue, green

abc is tricolored

lines ab, bc, ac are 2-colored

Sperner's Lemma (1928)

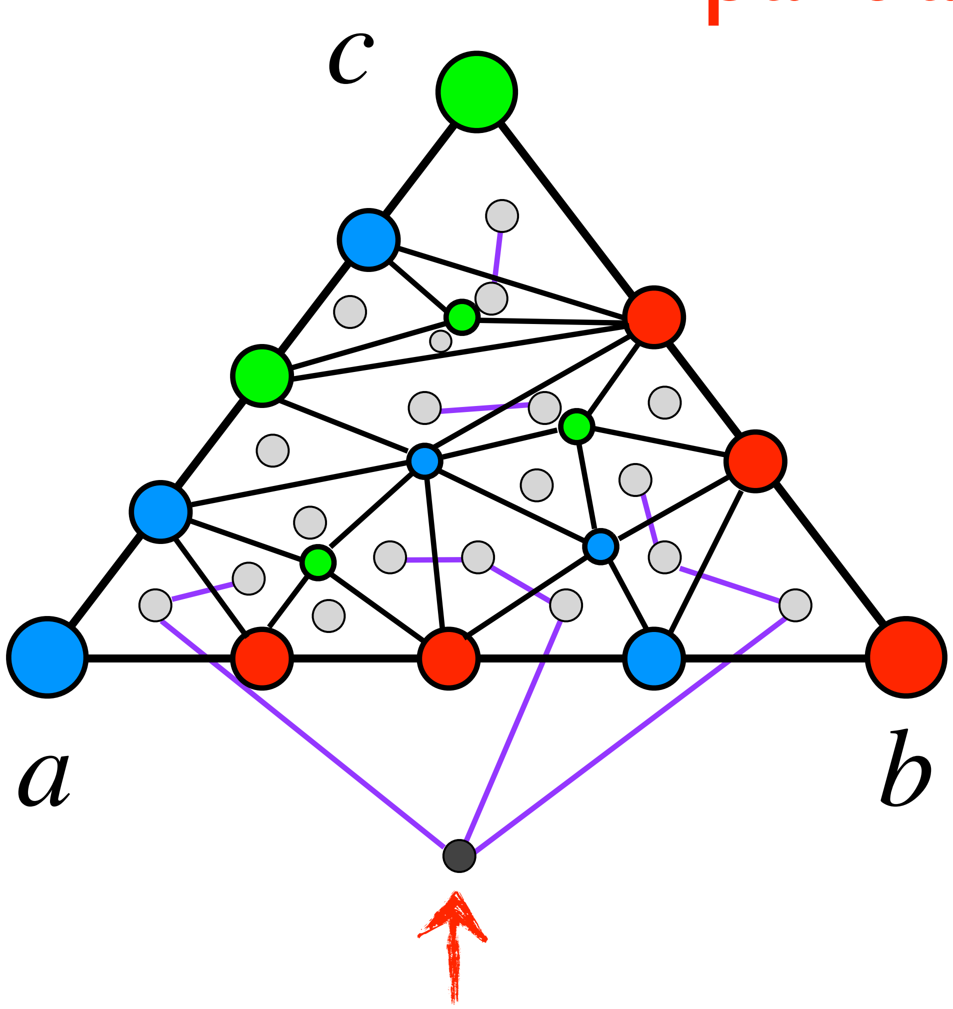
∀ properly colored triangulation of a triangle,

∃ a tricolored small triangle.

Sperner's Lemma (1928)

∀ properly colored triangulation of a triangle,
∃ a tricolored small triangle.

partial dual graph:



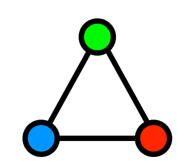
degree is odd

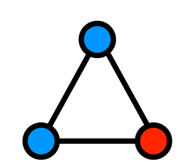
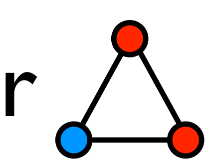
each △ is a vertex

the outer-space is a vertex

add an edge if 2 △

share a  edge

degree of  node: 1

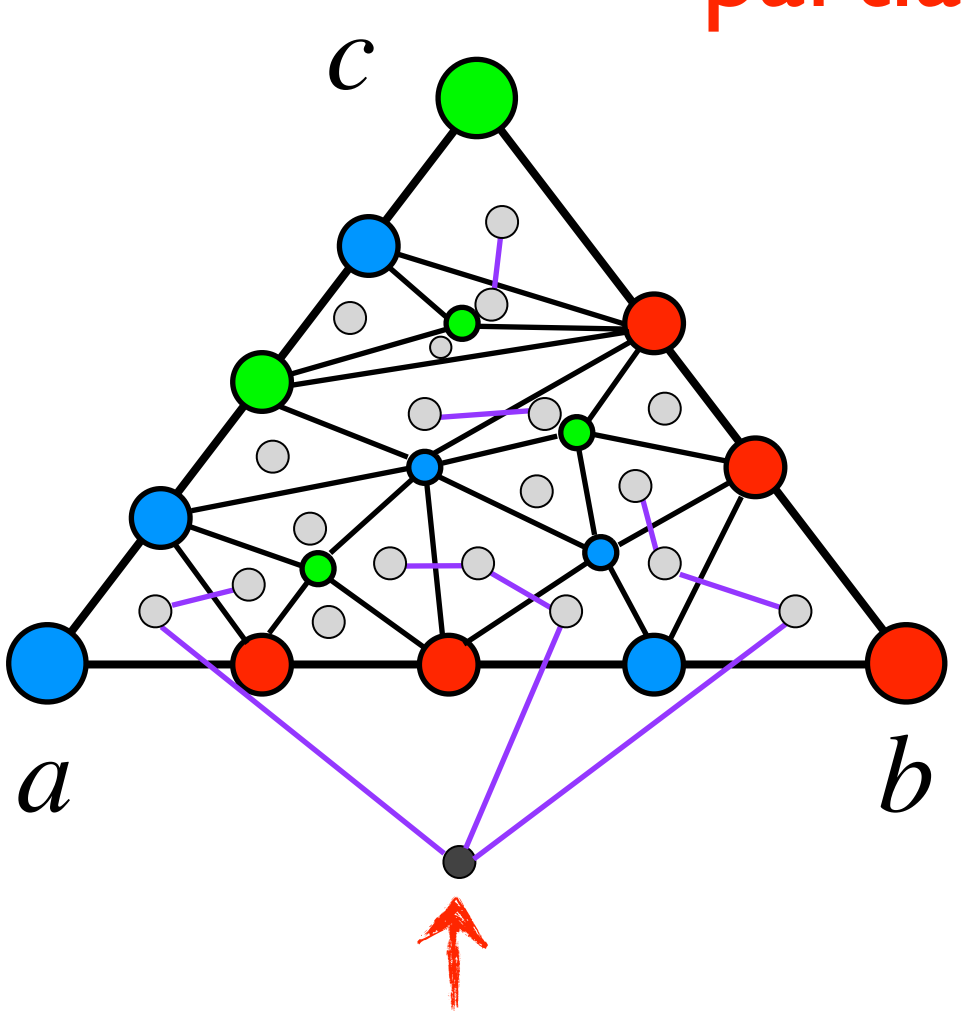
degree of  or  node: 2

other cases: 0 degree

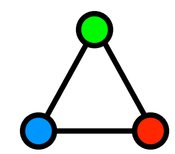
Sperner's Lemma (1928)

∀ properly colored triangulation of a triangle,
∃ a tricolored small triangle.

partial dual graph:



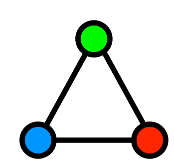
degree is odd

degree of  node: 1

degree of other △: even

handshaking lemma:

\# of odd-degree vertices is even.

\# of  : odd $\neq 0$

Sperner's Lemma (1928)

∀ properly colored triangulation of a triangle,
∃ a tricolored small triangle.

high-dimension: triangle ⇨ simplex

triangulation ⇨ simplicial subdivision

Brouwer's fixed point theorem (1911)

∀ continuous function f: $B \to B$ of an n-dimensional ball B, ∃ a fixed point $x = f(x)$.

Pigeonhole Principle

If $> mn$ objects are partitioned into n classes, then some class receives $> m$ objects.

Schubfachprinzip

"drawer principle"

Dirichlet Principle

Johann Peter Gustav Lejeune Dirichlet

Dirichlet's approximation

x is an irrational number.

Approximate *x* by a rational
with bounded denominator.

Theorem (Dirichlet 1879)

For any natural number n, there is a rational number $\frac{p}{q}$ such that $1 \leq q \leq n$ and

$$\left| x - \frac{p}{q} \right| < \frac{1}{nq}.$$

x is an irrational number.

Theorem (Dirichlet 1879)

For any natural number n, there is a rational number $\frac{p}{q}$ such that $1 \le q \le n$ and

$$\left| x - \frac{p}{q} \right| < \frac{1}{nq}.$$

fractional part: $\{x\} = x - \lfloor x \rfloor$

$(n+1)$ pigeons: $\{kx\}$ for $k = 1, \ldots, n+1$

n holes: $\left(0, \frac{1}{n}\right), \left(\frac{1}{n}, \frac{2}{n}\right), \ldots, \left(\frac{n-1}{n}, 1\right)$

x is an irrational number.

fractional part: $\{x\} = x - \lfloor x \rfloor$

$(n+1)$ pigeons: $\{kx\}$ for $k = 1, \ldots, n+1$

n holes: $\left(0, \frac{1}{n}\right), \left(\frac{1}{n}, \frac{2}{n}\right), \ldots, \left(\frac{n-1}{n}, 1\right)$

$\exists 1 \leq b < a \leq n+1 \quad \{ax\}, \{bx\}$ in the same hole

$$|(a-b)x - (\lfloor ax \rfloor - \lfloor bx \rfloor)| = |\{ax\} - \{bx\}| < \frac{1}{n}$$

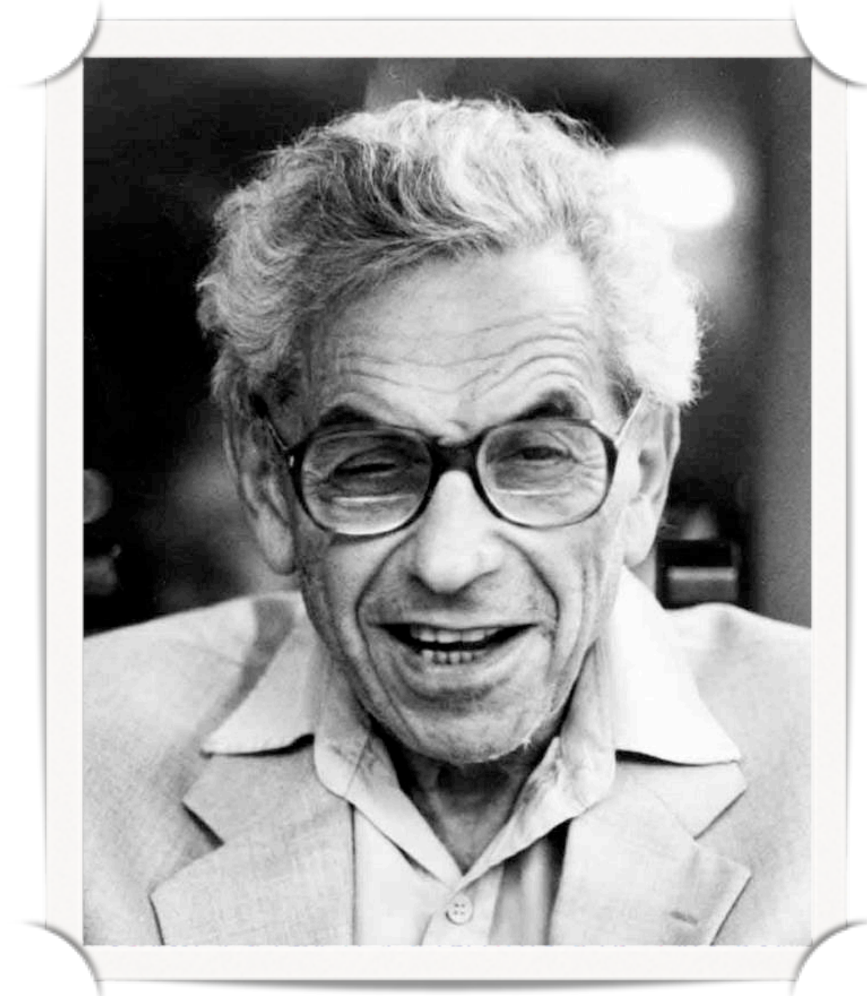
integers: $q \leq n$ $\quad p$

$$|qx - p| < \frac{1}{n} \quad \Rightarrow \quad \left| x - \frac{p}{q} \right| < \frac{1}{nq}.$$

An *initiation* question to Mathematics

$\forall S \subseteq \{1, 2, \ldots, 2n\}$ that $|S| > n$

$\exists a, b \in S$ such that $a \mid b$



Paul Erdős

$\forall a \in \{1, 2, \ldots, 2n\}$

$a = 2^k m$ for an odd m

$C_m = \{2^k m \mid k \geq 0, 2^k m \leq 2n\}$

$>n$ pigeons: S

n pigeonholes: $C_1, C_3, C_5, \ldots, C_{2n-1}$

$a < b \quad a, b \in C_m \quad \Rightarrow \quad a \mid b$

Monotonic subsequences

sequence: $(a_1, \ldots, a_n)$ of *n* different numbers

$1 \leq i_1 < i_2 < \cdots < i_k \leq n$

subsequence:

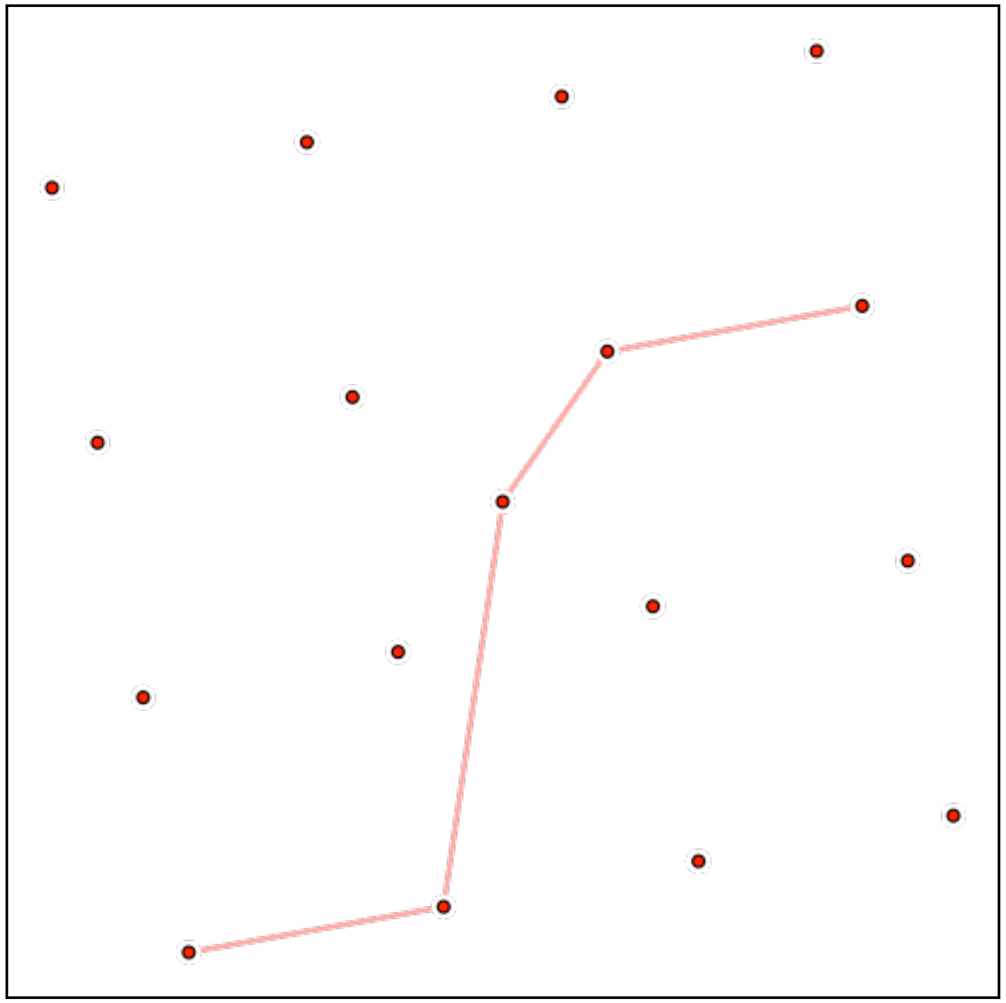
$$(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$$

increasing:

$$a_{i_1} < a_{i_2} < \ldots < a_{i_k}$$

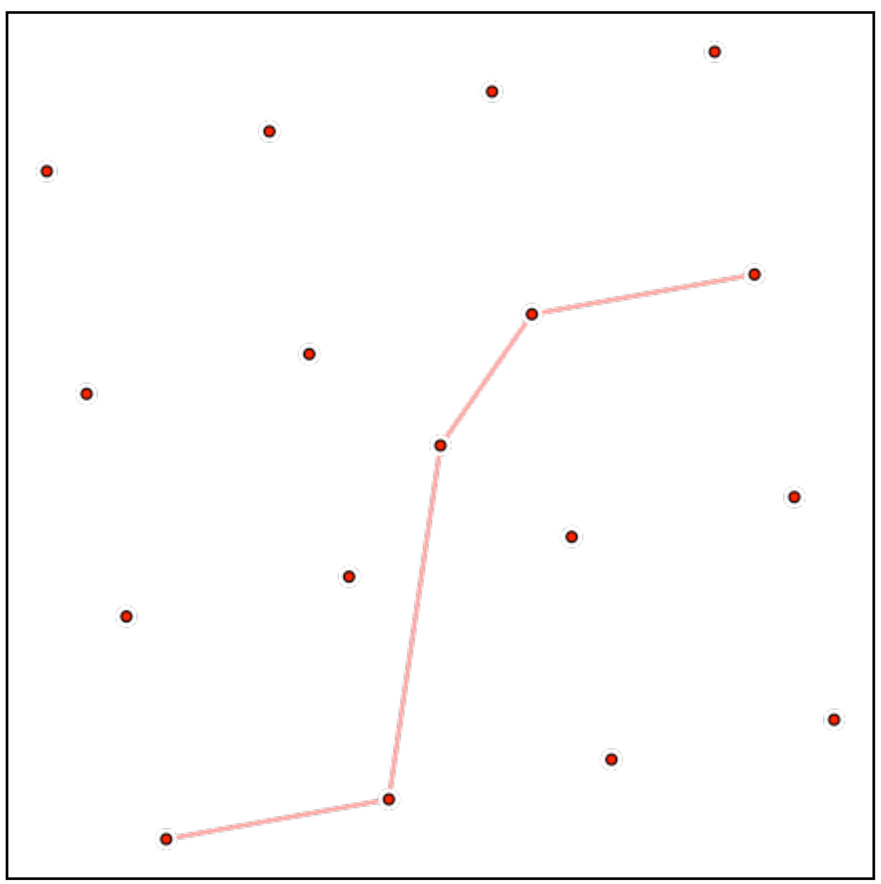
decreasing:

$$a_{i_1} > a_{i_2} > \ldots > a_{i_k}$$



Theorem (Erdős-Szekeres 1935)

A sequence of $> mn$ different numbers must contain either an increasing subsequence of length $m+1$, or a decreasing subsequence of length $n+1$.



$(a_1, \ldots, a_N)$ of *N* different numbers $\quad N > mn$

associate each a_i with (x_i, y_i)

x_i : length of longest *increasing* subsequence *ending* at a_i

y_i : length of longest *decreasing* subsequence *starting* at a_i

$$\forall i \neq j, \quad (x_i, y_i) \neq (x_j, y_j)$$

assume $i<j$

Cases.1: $a_i < a_j \Rightarrow x_i < x_j$

Cases.2: $a_i > a_j \Rightarrow y_i > y_j$

$(a_1, \ldots, a_N)$ of *N* different numbers $N > mn$

x_i : length of longest *increasing* subsequence *ending* at a_i

y_i : length of longest *decreasing* subsequence *starting* at a_i

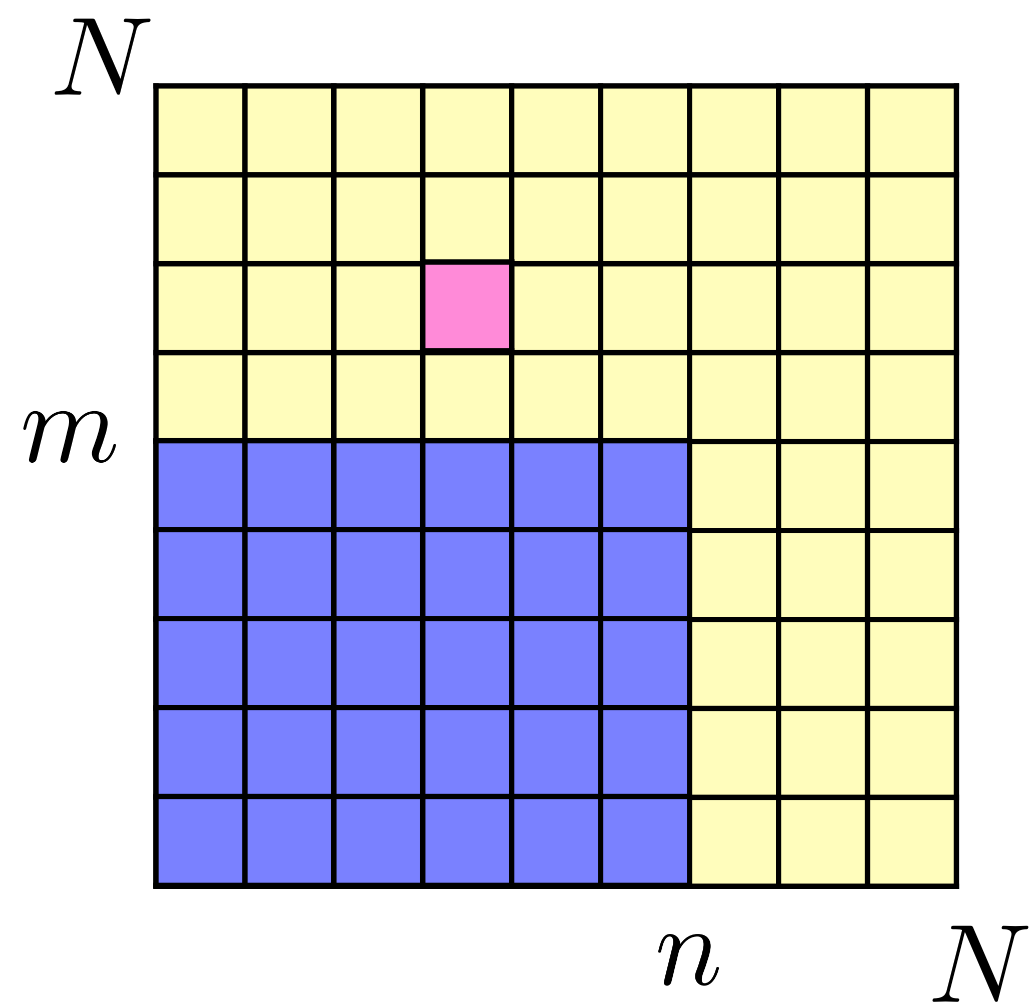
$$\forall i \neq j, \quad (x_i, y_i) \neq (x_j, y_j)$$

"One pigeon per each hole."

No way to put *N* pigeons into *mn* holes.

"N pigeons" $(a_1, \ldots, a_N)$

a_i is in hole (x_i, y_i)



Theorem (Erdős-Szekeres 1935)

A sequence of $> mn$ different numbers must contain either an increasing subsequence of length $m+1$, or a decreasing subsequence of length $n+1$.

$(a_1, \ldots, a_N)$ $\quad N > mn$

x_i : length of longest *increasing* subsequence *ending* at a_i

y_i : length of longest *decreasing* subsequence *starting* at a_i