Counting Argument
Circuit Complexity

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

- **DAG** (directed acyclic graph)
- Nodes:
  - inputs: \( x_1, \ldots, x_n \)
  - gates: \( \land, \lor, \neg \)
- Complexity: \#gates
**Theorem** (Shannon 1949)

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

\[ \left| \{0,1\}^n \rightarrow \{0,1\} \right| = 2^{2^n} \]

# of circuits with \( t \) gates:

\(< 2^t(2n + t + 1)^{2t} \]

De Morgan’s law:

\[ \neg (A \lor B) = \neg A \land \neg B \]
\[ \neg (A \land B) = \neg A \lor \neg B \]

\( x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n, 0, 1 \)

\( \land, \lor \) gates

\( \land, \lor \)

other \((t-1)\) gates
Theorem (Shannon 1949)

Almost all

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

One circuit computes one function

\[ \#f \text{ computable by } t \text{ gates} \leq \]
\[ \#\text{circuits with } t \text{ gates} \leq \]
\[ < 2^t(2n + t + 1)^{2t} \ll 2^{2n} = \#f \]

for \( t \leq \frac{2^n}{3n} \)
Double Counting

“Count the same thing twice. The result will be the same.”

<table>
<thead>
<tr>
<th>sum by row</th>
<th>sum by column</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A )</td>
<td>( B )</td>
</tr>
</tbody>
</table>

\[ A = B \]
Handshaking Lemma

A party of $n$ guests.

Handshaking Lemma: The number of people who shake an odd number of other people's hands is even.

Represented by graph:

$n$ guests $\Leftrightarrow$ $n$ vertices
handshaking $\Leftrightarrow$ edge
# of handshaking $\Leftrightarrow$ degree
Handshaking Lemma (Euler 1736)

\[ \sum_{v \in V} d(v) = 2|E| \]
Handshaking Lemma (Euler 1736)

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

Count the # of edge orientations:

\[ (u, v) : \{u, v\} \in E \]

Count by vertex:

\[ \forall v \in V \]

\[ d \text{ directed edges} \]

\[ (v, u_1) \cdots (v, u_d) \]

Count by edge:

\[ \forall \{u, v\} \in E \]

\[ 2 \text{ orientations} \]

\[ (u, v) \text{ and } (v, u) \]
Handshaking 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

$ab$ are colored differently

$\exists$ small segment

Emanuel Sperner (1905–1980)
Sperner’s Lemma

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

Sperner’s Lemma (1928)
**Sperner’s Lemma** (1928)

\(\forall\) properly colored triangulation of a triangle,
\(\exists\) a properly colored small triangle.

**Partial dual graph:**
- Each \(\triangle\) is a vertex.
- The outer-space is a vertex.
- Add an edge if 2 \(\triangle\)s share a \(\triangle\) edge.
- Degree of \(\triangle\) node: 1
- Degree of \(\triangle\) or \(\triangle\) node: 2
- Other cases: 0 degree

Degree is odd.
Sperner’s Lemma (1928)
∀ a properly colored triangulation of a triangle,
∃ a properly colored small triangle.

partial dual graph:

degree of \( \Delta \) node: 1
degree of other \( \Delta \): even

handshaking lemma:
# of odd-degree vertices is even.

# of \( \Delta \): odd \( \neq 0 \)
**Brouwer's fixed point theorem** *(1911)*

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

**Sperner’s Lemma** *(1928)*

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

**high-dimension:**

triangle $\rightarrow$ simplex

triangulation $\rightarrow$ simplicial subdivision
Averaging Principle
Pigeonhole Principle

“$n + 1$ pigeons cannot sit in $n$ holes so that every pigeon is alone in its hole.”
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
(1805 – 1859)
Dirichlet's approximation

Approximate any **irrational** $x$
by a **rational** with **bounded denominator**.

**Theorem (Dirichlet 1879)**

\[
\forall \text{ irrational } x \text{ and natural number } n, \ \exists \text{ a rational } \frac{p}{q}
\text{ such that } 1 \leq q \leq n \text{ and }
\left| x - \frac{p}{q} \right| < \frac{1}{nq}
\]
Theorem (Dirichlet 1879)

\[ \forall \text{irrational } x \text{ and natural number } n, \exists \text{ a rational } \frac{p}{q} \text{ such that } 1 \leq q \leq n \text{ and } \]

\[ \left| x - \frac{p}{q} \right| < \frac{1}{nq} \iff \left| qx - p \right| < \frac{1}{n} \]

fractional part: \( \{x\} = x - \lfloor x \rfloor \)

\((n + 1)\) pigeons: \( \{kx\} \) for \( k = 1, 2, \ldots, n + 1 \)

\(n\) holes: \( \left( 0, \frac{1}{n} \right), \left( \frac{1}{n}, \frac{2}{n} \right), \ldots, \left( \frac{n-1}{n}, 1 \right) \)
fractional part: \( \{x\} = x - \lfloor x \rfloor \)

\((n + 1)\) pigeons: \( \{kx\} \) for \( k = 1, 2, \ldots, n + 1 \)

\(n\) 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: \( q \leq n \)

\[ |qx - p| < \frac{1}{n} \quad \Rightarrow \quad \left| x - \frac{p}{q} \right| < \frac{1}{nq}. \]
An initiation question to Mathematics

\[ \forall S \subseteq \{1, 2, \ldots, 2n\} \quad \text{that} \quad |S| > n \]
\[ \exists a, b \in S \quad \text{such that} \quad a \mid b \]

\[ \forall a \in \{1, 2, \ldots, 2n\} \]
\[ a = 2^k m \quad \text{for an odd} \quad m \]

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

\[ >n \quad \text{pigeons:} \quad S \]
\[ n \quad \text{pigeonholes:} \quad C_1, C_3, C_5, \ldots, C_{2n-1} \]

\[ a < b \quad a, b \in C_m \quad \rightarrow \quad a \mid b \]
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:

\[a_{i_1} < a_{i_2} < \cdots < a_{i_k}\]

decreasing:

\[a_{i_1} > a_{i_2} > \cdots > a_{i_k}\]
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 \(N > mn\)

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 \(a_i\)

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

assume \(i < j\)

**Cases.1:** \(a_i < a_j\) => \(x_i < x_j\)

**Cases.2:** \(a_i > a_j\) => \(y_i > y_j\)
\((a_1, \ldots, a_N)\) of \(N\) different numbers \quad \(N > mn\)

\(x_i\) : length of longest *increasing* subsequence *ending* at \(a_i\)

\(y_i\) : length of longest *decreasing* subsequence *starting* at \(a_i\)

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

“One pigeon per each hole.”

No way to put \(N\) pigeons into \(mn\) holes.

\(\text{“N pigeons” } (a_1, \ldots, a_N)\)

\(a_i\) 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 \( a_i \)