Combinatorics

南京大学
尹一通
Circuit Complexity

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

- **Boolean circuit**

- **Nodes:**
  - inputs: $x_1 \ldots x_n$
  - gates: $\land \lor \neg$

- **Complexity:** #gates

- **DAG** (directed acyclic graph)
**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 \textit{f} : \{0, 1\}^n \rightarrow \{0, 1\}

\# of circuits with \(t\) gates:

\[\land, \lor\ \text{gates}\]

\[x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n, 0, 1\]

De Morgan’s law:

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

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

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

\[\land, \lor\]

other \((t-1)\) gates

\[x_i, \neg x_i, 0, 1\]
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.

**Theorem (Shannon 1949)**

Almost all functions $f$ computable by $t$ gates are computed by circuits with $2^t (2n + t + 1)^{2t} \ll 2^{2^n}$, so

$$t = \frac{2^n}{3n}$$
Double Counting

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

A party of $n$ guests.

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

Modeling:

$n$ guests $\Leftrightarrow$ $n$ vertices
handshaking $\Leftrightarrow$ edge

$\#$ of handshaking $\Leftrightarrow$ degree
Lemma (Euler 1736)

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

In the 1736 paper of Seven Bridges of Königsberg

Leonhard Euler
**Lemma (Euler 1736)**

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

**Count directed edges:**

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

**Count by vertex:**

\[ \forall v \in V \]

\[ d \text{ directed edges} \]

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

**Count by edge:**

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

\[ 2 \text{ directions} \]

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

\[ a \quad b \]

\( ab \) have different color

\( \exists \) small segment

Emanuel Sperner
Sperner’s Lemma

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

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

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

partial dual graph:
- each \( \triangle \) is a vertex
- the outer-space is a vertex
- add an edge if 2 \( \triangle \) share a edge

degree of \( \triangle \) node: 1
degree of \( \triangle \) or \( \triangle \) node: 2
other cases: 0 degree
**Sperner’s Lemma (1928)**

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

**Partial dual graph:**

degree of $\triangle$ node: 1

degree of other $\triangle$: even

**Handshaking lemma:**

# of odd-degree vertices is even.

# of $\triangle$: odd ≠ 0
Sperner’s Lemma (1928)
\[ \forall \text{ properly colored triangulation of a triangle,} \]
\[ \exists \text{ a tricolored small triangle.} \]

Brouwer’s fixed point theorem (1911)
\[ \forall \text{ continuous function } f : B \rightarrow B \text{ of an} \]
\[ n\text{-dimensional ball } B, \exists \text{ a fixed point } x = f(x). \]

high-dimension: triangle $\rightarrow$ simplex

triangulation $\rightarrow$ simplicial subdivision
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

$$\left| x - \frac{p}{q} \right| < \frac{1}{nq}.$$
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 $1 \leq q \leq n$ 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:** \(0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1\)
$x$ is an irrational number.

**fractional part:**  \[ \{x\} = x - \lfloor x \rfloor \]

**(n+1) pigeons:**  \[ \{kx\} \text{ for } k = 1, \ldots, n + 1 \]

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

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

\[ (a - b)x - ([ax] - [bx]) = \{ax\} - \{bx\} < \frac{1}{n} \]

**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

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

\[ \forall a \in \{1, 2, \ldots, 2n\} \]

\[ a = 2^k m \quad \text{for an odd} \quad m \]

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

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

\[ a < b \quad a, b \in C_m \quad \Rightarrow \quad a \mid b \]
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 \textit{increasing}\ subsequence \textit{ending} at \(a_i\)

\(y_i:\) length of longest \textit{decreasing}\ subsequence \textit{starting} at \(a_i\)

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

assume \(i < j\)

\textbf{Cases.1:} \(a_i < a_j\) \quad \Rightarrow \quad x_i < x_j\)

\textbf{Cases.2:} \(a_i > a_j\) \quad \Rightarrow \quad y_i > y_j\)
\((a_1, \ldots, a_N)\) of \(N\) different numbers \(N > mn\)

\(x_i: \) length of longest \textit{increasing} subsequence \textit{ending} at \(a_i\)

\(y_i: \) length of longest \textit{decreasing} subsequence \textit{starting} at \(a_i\)

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

“\(N\) pigeons” \((a_1, \ldots, a_N)\)

\(a_i\) is in hole \((x_i, y_i)\)

“\textit{One pigeon per each hole.”}”

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