m-intersections

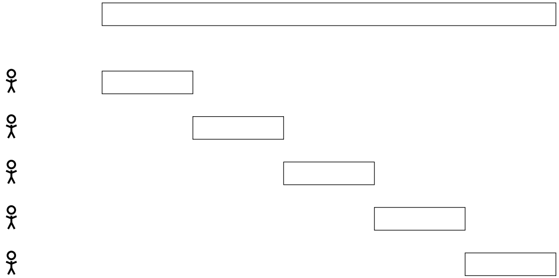
Taehyun Eom

KAIST

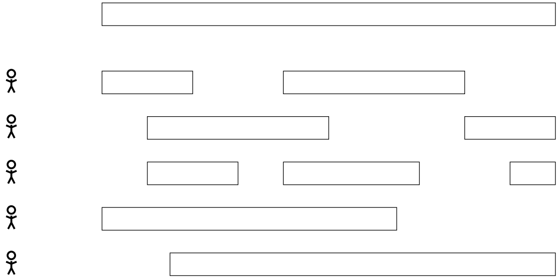
2022.06.30

Secret Sharing

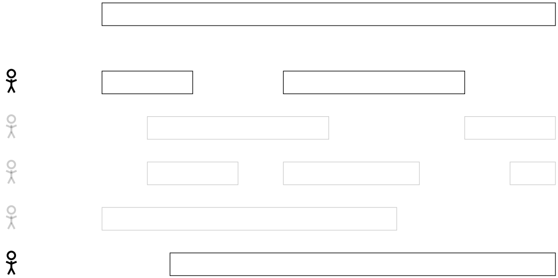
Secret Sharing



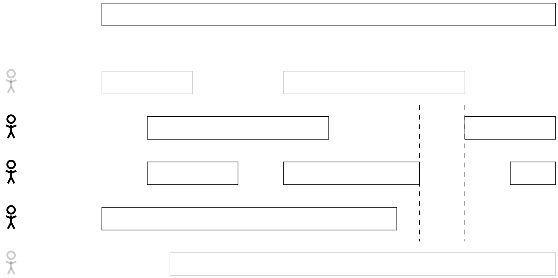
Secret Sharing



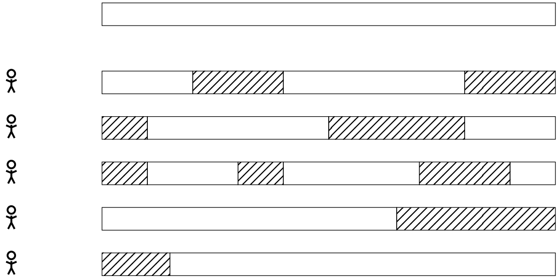
Secret Sharing



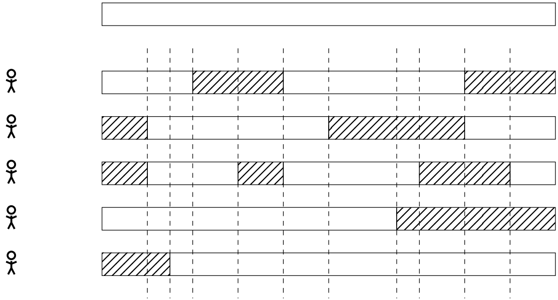
Secret Sharing

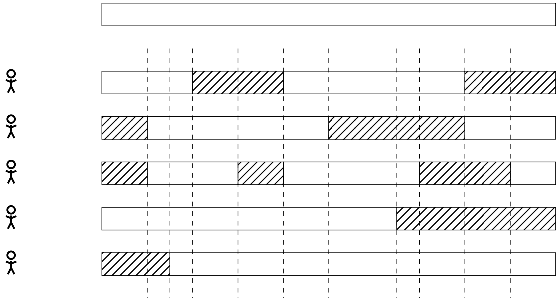


Secret Sharing



Secret Sharing





To be recovered by every choice of m people

$\Leftrightarrow$ number of shaded area $\leq (m-1)$ for each part.

Measure theoretic statement

Proposition

Let Ω be the measurable space with measure μ. Then, suppose measurable subsets $A_1, \cdots, A_n$ of Ω satisfies

$$\sigma_m := \sum_{1 \le i_1 < i_2 < \cdots < i_m \le n} \mu(A_{i_1} \cap \cdots \cap A_{i_m}) = 0.$$

Then,

$$\sum_i \mu(A_i) \le (m-1)\mu(\Omega).$$

In other words,

Proposition

$\sigma_m = 0$ implies $\sigma_1 \le (m-1)\sigma_0$.

Measure theoretic proof

Overlapping Theorem

Let $(\Omega, \mathbb{P})$ be a probability space, and $E_1, \cdots, E_n$ be events. If we define a convex continuous function

$$Q_m(x) := \binom{\lfloor x \rfloor}{m} + \binom{\lfloor x \rfloor}{m-1} \langle x \rangle = \binom{\lfloor x \rfloor}{m} \langle x \rangle + \binom{\lfloor x \rfloor + 1}{m} (1 - \langle x \rangle),$$

we have

$$\sum_{1 \le i_1 < i_2 < \cdots < i_m \le n} \mathbb{P}(E_{i_1} \cap \cdots \cap E_{i_m}) \ge Q_m \left(\sum_{i=1}^{n} \mathbb{P}(E_i) \right).$$

This theorem is the Theorem 1.1 from *Javier Cilleruelo, Gérald Tenenbaum, An overlapping theorem with applications, 2006*.

Combinatorial version of the overlapping theorem

Overlapping Theorem

- For any $s \geq 0$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0)$.

Combinatorial version of the overlapping theorem

Overlapping Theorem

- For any $s \geq 0$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s \geq 1$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s-1}{m-1}(\sigma_1 - s\sigma_0)$.

Combinatorial version of the overlapping theorem

Overlapping Theorem

- For any $s \geq 0$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s \geq 1$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s-1}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s > m \geq 0$, $\sigma_m \leq \frac{1}{m+1}\binom{s}{m}\sigma_0 + \frac{m}{s-m}\sigma_{m+1}$.

Combinatorial version of the overlapping theorem

Overlapping Theorem

- For any $s \geq 0$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s \geq 1$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s-1}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s > m \geq 0$, $\sigma_m \leq \frac{1}{m+1}\binom{s}{m}\sigma_0 + \frac{m}{s-m}\sigma_{m+1}$.
- For any $s > m \geq 1$, $\sigma_m \leq \frac{1}{m^2}\binom{s}{m-1}\sigma_1 + \frac{m^2-1}{m(s-m+1)}\sigma_{m+1}$.

Combinatorial version of the overlapping theorem

Overlapping Theorem

- For any $s \geq 0$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s \geq 1$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s-1}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s > m \geq 0$, $\sigma_m \leq \frac{1}{m+1}\binom{s}{m}\sigma_0 + \frac{m}{s-m}\sigma_{m+1}$.
- For any $s > m \geq 1$, $\sigma_m \leq \frac{1}{m^2}\binom{s}{m-1}\sigma_1 + \frac{m^2-1}{m(s-m+1)}\sigma_{m+1}$.
- For any $s \geq 0$ and $m \geq p \geq 1$,

$$\sigma_m \geq \binom{s}{m}\sigma_0 + \frac{\binom{s}{m-1}}{\binom{s}{p-1}}\left(\sigma_1 - \binom{s}{p}\sigma_0\right).$$

Combinatorial version of the overlapping theorem

Overlapping Theorem

- For any $s \geq 0$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s \geq 1$ and $m \geq 1$, $\sigma_m \geq \binom{s}{m}\sigma_0 + \binom{s-1}{m-1}(\sigma_1 - s\sigma_0)$.
- For any $s > m \geq 0$, $\sigma_m \leq \frac{1}{m+1}\binom{s}{m}\sigma_0 + \frac{m}{s-m}\sigma_{m+1}$.
- For any $s > m \geq 1$, $\sigma_m \leq \frac{1}{m^2}\binom{s}{m-1}\sigma_1 + \frac{m^2-1}{m(s-m+1)}\sigma_{m+1}$.
- For any $s \geq 0$ and $m \geq p \geq 1$,

$$\sigma_m \geq \binom{s}{m}\sigma_0 + \frac{\binom{s}{m-1}}{\binom{s}{p-1}}\left(\sigma_1 - \binom{s}{p}\sigma_0\right).$$

If we set $s = \lfloor \frac{\sigma_1}{\sigma_0} \rfloor$, the first inequality gives the overlapping theorem.

Proof

Let $\beta_m = \mu(\{x \in \Omega \mid \#\{i \mid x \in A_i\} = m\})$. Then, by simple counting, we have $\sigma_m = \sum_k \binom{k}{m} \beta_k$.

Proof

Let $\beta_m = \mu(\{x \in \Omega \mid \#\{i \mid x \in A_i\} = m\})$. Then, by simple counting, we have $\sigma_m = \sum_k \binom{k}{m} \beta_k$.
Now, for any $r > s \geq 0$ and $m \geq 1$, we have

$$(r-s)\binom{s}{m-1} \leq \binom{r}{m} - \binom{s}{m} \leq (r-s)\binom{r-1}{m-1}$$

Proof

Let $\beta_m = \mu(\{x \in \Omega \mid \#\{i \mid x \in A_i\} = m\})$. Then, by simple counting, we have $\sigma_m = \sum_k \binom{k}{m} \beta_k$.
Now, for any $r > s \geq 0$ and $m \geq 1$, we have

$$(r-s)\binom{s}{m-1} \leq \binom{r}{m} - \binom{s}{m} \leq (r-s)\binom{r-1}{m-1}$$

Hence, for fixed $s \geq 0$ and $m \geq 1$, we have

$$\sigma_m = \sum_k \binom{k}{m} \beta_k \geq \sum_k \left(\binom{s}{m} + (k-s)\binom{s}{m-1} \right) \beta_k$$

Proof

Let $\beta_m = \mu(\{x \in \Omega \mid \#\{i \mid x \in A_i\} = m\})$. Then, by simple counting, we have $\sigma_m = \sum_k \binom{k}{m} \beta_k$.
Now, for any $r > s \geq 0$ and $m \geq 1$, we have

$$(r-s)\binom{s}{m-1} \leq \binom{r}{m} - \binom{s}{m} \leq (r-s)\binom{r-1}{m-1}$$

Hence, for fixed $s \geq 0$ and $m \geq 1$, we have

$$\begin{aligned}\sigma_m = \sum_k \binom{k}{m} \beta_k &\geq \sum_k \left(\binom{s}{m} + (k-s)\binom{s}{m-1}\right)\beta_k \\ &= \binom{s}{m}\sum_k \beta_k + \binom{s}{m-1}\left(\sum_k k\beta_k - s\sum_k \beta_k\right)\end{aligned}$$

Proof

Let $\beta_m = \mu(\{x \in \Omega \mid \#\{i \mid x \in A_i\} = m\})$. Then, by simple counting, we have $\sigma_m = \sum_k \binom{k}{m}\beta_k$.
Now, for any $r > s \geq 0$ and $m \geq 1$, we have

$$(r-s)\binom{s}{m-1} \leq \binom{r}{m} - \binom{s}{m} \leq (r-s)\binom{r-1}{m-1}$$

Hence, for fixed $s \geq 0$ and $m \geq 1$, we have

$$\begin{aligned}
\sigma_m = \sum_k \binom{k}{m}\beta_k &\geq \sum_k \left(\binom{s}{m} + (k-s)\binom{s}{m-1}\right)\beta_k \\
&= \binom{s}{m}\sum_k \beta_k + \binom{s}{m-1}\left(\sum_k k\beta_k - s\sum_k \beta_k\right) \\
&= \binom{s}{m}\sigma_0 + \binom{s}{m-1}(\sigma_1 - s\sigma_0).
\end{aligned}$$