Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

For all x, $1 - x \leq e^{-x}$. See here.

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

For all x, $1 - x \leq e^{-x}$. See here.

$\Pr[\text{NoColl}_q] \leq \prod_{i=1}^{q-1} e^{-i/N}$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

For all x, $1 - x \leq e^{-x}$. See here.

$\Pr[\text{NoColl}_q] \leq \prod_{i=1}^{q-1} e^{-i/N} = e^{-\sum(i/N)}$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

For all x, $1 - x \leq e^{-x}$. See here.

$\Pr[\text{NoColl}_q] \leq \prod_{i=1}^{q-1} e^{-i/N} = e^{-\sum(i/N)} = e^{-q(q-1)/2N}$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

For all x, $1 - x \leq e^{-x}$. See here.

$\Pr[\text{NoColl}_q] \leq \prod_{i=1}^{q-1} e^{-i/N} = e^{-\sum(i/N)} = e^{-q(q-1)/2N}$

$\Pr[\text{Coll}] = 1 - \Pr[\text{NoColl}_q] \geq 1 - e^{-q(q-1)/2N}$

Birthday Paradox

Lemma (Lower bound from Katz and Lindell)

For any positive integer N, and $q \leq \sqrt{2N}$, let $y_1, \ldots, y_q$ be elements chosen uniformly and independently at random from a set of size N. The probability that there exists distinct i and j such that $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$

Let NoColl_i bet the event that there are no collisions among $y_1, \ldots, y_i$.
NoColl_q is the event that there are no collisions at all.

If NoColl_q occurs, then NoColl_i occurs for every $i < q$.
$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}]$

$\Pr[\text{NoColl}_i \mid \text{NoColl}_{i-1}] = 1 - \frac{i}{N}$

$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1} (1 - \frac{i}{N})$

For all x, $1 - x \leq e^{-x}$. See here.

$\Pr[\text{NoColl}_q] \leq \prod_{i=1}^{q-1} e^{-i/N} = e^{-\sum(i/N)} = e^{-q(q-1)/2N}$

$\Pr[\text{Coll}] = 1 - \Pr[\text{NoColl}_q] \geq 1 - e^{-q(q-1)/2N} \geq 1 - (1 - \frac{q(q-1)}{4N}) = \frac{q(q-1)}{4N}$

$e^{-x} \leq 1 - \frac{x}{2}$