Min-entropy

Last modified: 2026-11-12 01:15:28 (PST)

The entropy of a random variable averages its surprisal. Other summaries of its probabilities answer other questions. This page adds the smallest of them, the min-entropy, to the collision entropy.

Min-entropy

Definition 0.1 (Min-entropy)**.** The **min-entropy** of a discrete random variable X is the logarithm of the reciprocal of the largest probability that X takes any one value:

$$\mathbb{H}_\infty(X) = -\log \max_x \mathbb{P}(X = x).$$

It is the limiting case of the Rényi entropy of order α (Rényi 1961), which approaches it as $\alpha \to \infty$.

Example 0.1 (Min-entropy of a three-valued random variable)**.**
Let X take three values with probabilities 1/2, 1/4 and 1/4. The R chunk below finds the largest probability and the min-entropy, with base-2 logarithms.

```
p <- c(1 / 2, 1 / 4, 1 / 4)
max_prob <- max(p)
min_entropy <- -log2(max_prob)
c(max_prob = max_prob, min_entropy = min_entropy)
#>    max_prob min_entropy
#>         0.5         1.0
```

The largest probability is 0.5, so the min-entropy is $\mathbb{H}_\infty(X) = 1$ bit.

Theorem 0.1 (The min-entropy is at most the collision entropy)**.** *Let X be a discrete random variable. Then the min-entropy is at most the collision entropy:*

$$\mathbb{H}_\infty(X) \leq \mathbb{H}_2(X).$$

Proof

Proof. Let $p_{\max} = \max_x \mathbb{P}(X = x)$. Each probability $\mathbb{P}(X = x)$ is at most $p_{\max}$, so $\mathbb{P}(X = x)^2 \leq p_{\max}\,\mathbb{P}(X = x)$. Sum over the values x:

$$\sum_x \mathbb{P}(X = x)^2 \leq p_{\max} \sum_x \mathbb{P}(X = x).$$

The probabilities sum to 1, so the collision probability is at most $p_{\max}$:

$$\mathbb{P}(X = X') = \sum_x \mathbb{P}(X = x)^2 \leq p_{\max}.$$

The function $-\log$ is decreasing, so taking it of both sides flips the comparison:

$$-\log \mathbb{P}(X = X') \geq -\log p_{\max}.$$

The left side is $\mathbb{H}_2(X)$ and the right side is $\mathbb{H}_\infty(X)$. □

Example 0.2 (Three entropies of one random variable)**.**
The R chunk below computes the min-entropy, the collision entropy and the entropy of the random variable of Example 0.1.

```
p <- c(1 / 2, 1 / 4, 1 / 4)
min_entropy <- -log2(max(p))
collision_entropy <- -log2(sum(p^2))
shannon_entropy <- -sum(p * log2(p))
c(
  min_entropy = min_entropy,
  collision_entropy = collision_entropy,
  shannon_entropy = shannon_entropy
)
#>       min_entropy collision_entropy   shannon_entropy
#>          1.000000          1.415037          1.500000
```

The values rise from 1 to 1.415 to 1.5 bits, as Theorem 0.1 and the collision entropy bound say.

Remark 0.1 (Min-entropy measures the chance of a single guess). The best single guess at the value of X is its most probable value, and that guess is right with probability $2^{-\mathbb{H}_\infty(X)}$. So a min-entropy of k bits says that no guess succeeds with probability above 2^{-k}. The entropy gives no such guarantee, because it can be large while one value is very likely. That is why min-entropy is the measure of a secret's unpredictability.

References

Rényi, Alfréd. 1961. "On Measures of Entropy and Information." In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, edited by Jerzy Neyman. University of California Press. https://projecteuclid.org/euclid.bsmsp/1200512181.