Chapter 9

Equivalence of the Two Entropies

We show that the rival definitions of algorithmic entropy, $H(s)$ and $h(s)$, are in fact equivalent.

Theorem 9.1.

$$h(s) = H(s) + O(1).$$

More precisely, there exists a contant C independent of s such that

$$h(s) \leq H(s) \leq h(s) + C$$

for all $s \in \mathbb{S}$.

Proof ▶. As we saw in Proposition 8.1,

$$h(s) \leq H(s).$$

We must show that there exists a constant C, dependent only on our choice of universal machine U, such that

$$H(s) \leq h(s) + C$$

for all strings $s \in \mathbb{S}$.

Lemma 1.

$$\sum_{s \in \mathbb{S}} 2^{-h_T(s)} \leq 1.$$

Proof ▶. Each p for which $T(p)$ is defined contributes to $h_T(s)$ for just one s. Hence

$$\begin{aligned}\sum_{s\in\mathbb{S}} 2^{-h_T(s)} &= \sum_{s\in\mathbb{S}} \left(\sum_{p:T(p)=s} 2^{-|s|} \right) \\ &= \sum_{p:T(p)\text{ defined}} 2^{-|s|} \\ &\leq 1,\end{aligned}$$

since the set of p for which $T(p)$ is defined is prefix-free.

Thus the numbers $h(s)$ satisfy Kraft's Inequality. However, we cannot apply the converse as it stands since these numbers are not in general integral.

We therefore set

$$h_s = [h(s)] + 1$$

for each string $s \in \mathbb{S}$. (Here $[x]$ denotes, as usual, the greatest integer $\leq x$.) Thus

$$h(s) < h_s \leq h(s) + 1.$$

Since

$$\sum 2^{-h_s} \leq \sum 2^{-h(s)} \leq 1,$$

the integers h_s, or rather the set of pairs

$$S = \{(s, h_s)\} \in \mathbb{S} \times \mathbb{N},$$

satisfy the first criterion of Chaitin's Lemma.

The Converse, if we could apply it, would allow us to construct a machine M such that

$$H_M(s) \leq h_s$$

for all s with $h_s < \infty$. It would follow from this that

$$\begin{aligned}H(s) &\leq H_M(s) + |\langle M \rangle| \\ &\leq h_s + O(1) \\ &\leq h(s) + O(1).\end{aligned}$$

Unfortunately, *we have no reason to suppose that the h_s are recursively enumerable*. We cannot therefore apply the Converse directly, since we have not shown that its second criterion is fulfilled.

Fortunately, a nimble side-step steers us round this obstacle.

Lemma 2. *Suppose T is a Turing machine. Then the set*

$$S' = \{(s, m) \in \mathbb{S} \times \mathbb{N} : h_T(s) > 2^{-m}\}$$

is recursively enumerable.

Proof ▶. We construct a machine M which runs as follows.

At the nth stage, M runs through all $2^{n+1} - 1$ strings p of length $\leq n$. For each such string p, M emulates T for n steps. If T halts within these n steps, with $s = T(p)$, a note is made of the pair $(s, |p|)$.

At the end of the nth stage, the accumulated total

$$\mathrm{P}'_T(s) = \sum_{|p| \leq n : T(p) = s} 2^{-|p|}$$

is calculated for each string s that has appeared; and for each new integer $m = m(s)$ for which

$$\mathrm{P}'_T(s) \geq 2^{-m}$$

the pair (s, m) is output.

(Note that as more inputs are considered, $\mathrm{P}'_T(s)$ is increasing, tending towards $\mathrm{P}_T(s)$. Thus m is decreasing, passing through integers $\geq h_T(s)$.)

Lemma 3. *With the notation of the last lemma,*

$$\sum_{s, m : (s,m) \in S'} 2^{-m} \leq 2.$$

Proof ▶. As we saw in the proof of the last Lemma, the $m = m(s)$ that arise for a given s are $\geq h_T(s)$. Hence their sum is

$$< h_T(s) \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = 2h_T(s).$$

Thus the sum for all s is

$$< 2 \sum_s h_T(s) \leq 2,$$

by Lemma 1.

Now we *can* apply the Converse to the set

$$S'' = \{(s, m + 1) : (s, m) \in S'\};$$

for we have shown in Lemma 3 that this set satisfies the first criterion, while we saw in Lemma 1 that it is recursively enumerable.

Thus we can construct a machine M with the property that for each $(s, m) \in S$ we can find a program p such that

$$M(p) = s, \quad |p| \leq h_s + 1.$$

It follows that

$$H_M(s) \leq h_s + 1;$$

and so, taking $T = U$,

$$\begin{aligned} H(s) &\leq H_M(s) + |\langle M \rangle| \\ &\leq h_s + |\langle M \rangle| \\ &= h_s + O(1) \\ &\leq h(s) + O(1). \end{aligned}$$

Summary

We have established that $H(s)$ and $h(s)$ are equivalent definitions of entropy. It is thus open to us to use whichever is more convenient for the problem in hand.