Notes on Introduction to Kolmogorov Complexity

Venkatesan Guruswami

October 20, 2004

These are informal lecture notes detailing material covered in the lecture on Tuesday, Oct 19, 2004.

1 Introduction

The aim of the subject of *Kolmogorov* or *Kolmogorov-Chaitin* or *descriptive* complexity is to develop the notion of the quantity of information in an object, or equivalent the "complexity" of an object as an absolute property of the object alone. This is similar to computability or complexity theory which studied the complexity of languages; here we wish to study the complexity of individual strings.

Intuition tells us that some objects are complicated and some others are simple. Consider the information content of the following two binary sequences:

$$\begin{aligned} A &= 0101010101010101010101010101010101010101 \\ B &= 1001110101011101011100011010111001111010 \end{aligned}$$

Intuitively, sequence A is "simple" and contains little information because it is just the pattern 01 repeated 20 times, and we can imagine "compressing" it. In contrast, the sequence B appears to contain more information, and it seems hard to conceive a description for it other than the bit sequence itself.

Taking a cue from this example, we will aim to define the information content of an object to be the size of its *smallest* description. Note that we may always describe an object by placing a copy of it directly into its description; in the above example we can describe B as a forty bit string. A description significantly shorter than the object implies that the information contained within the object can be compressed into a small volume, and so the amount of information cannot be very large. Therefore, the size of the *shortest* description determines the amount of information. Without loss of generality, we will model objects that we wish to describe as binary strings, and also use binary strings to represent their descriptions (in potentially compressed form). To make descriptions useful, we like them to be finite. Thus a description is just a finite binary string. The size of a description will simply be the length of the corresponding binary string.

However, we need to work more to develop this theory in a sensible way; specifically we need to agree upon a universal method for describing objects which is "fair" (and does not artificially favor some objects over others).

Consider the so-called Richard-Berry paradox, where we define a natural number as "the least natural number that cannot be described in less then twenty words". If this number does exist, we have just described it in 13 words, contradicting its definition. If such a natural number does not exist, then all natural numbers can be described in fewer than 20 words. This indicates that we need to be very careful about what we mean by the notion of "description".

2 Formalizing descriptions

Since we would like to be able to identify the object unambiguously from its description, we can abstract a *description method* as a partial function $f : \Sigma^* \to \Sigma^*$ (say, $\Sigma = \{0, 1\}$) that maps descriptions to objects. The complexity of an object (binary string) x under description method f, denoted $C_f(p)$, is defined as

$$C_f(p) = \min\{|p| : f(p) = x\} \ , \tag{1}$$

In other words, $C_f(p)$ is the length of the shortest string p that describes x (under description method f).

We would like the information content of x to be defined as an intrinsic property of x alone, and yet the above definition clearly depends on f. So what is needed is a universally agreed upon method f. But which description method f should we use or agree upon? Why should there be any choice of such an f at all upon which a robust theory can be based? After all, it is conceivable that some description methods could be partisan and artificially "favor" certain objects with very short descriptions for them. In such a case objects with small descriptions would not be intrinsically simple as we would like them to be.

3 Universal description method and Kolmogorov complexity

We will try to pick a description method which is the "best" in terms of the minimum description length of *all* strings. To formalize this, we need a definition. Let us say a (partial) function f minorizes g if there is a constant c such that *for all* x, we have

$$C_f(x) \le C_g(x) + c \ .$$

In other words, we need at most a constant additive overhead to describe any object under f compared to its shortest description under g. Now, we would like to use a *minimal* universal description method U which minorizes every other candidate description method, and then define the size of an object's smallest description under U as its "complexity".[1]

But why should such a best f that minorizes everything else exist? In fact, if we allow all possible partial functions as description methods, such an f *does not* exist! Here is a quick argument sketching why this is the case. Let f be any partial function. Take an infinite sequence of strings $p_1, p_2, \cdots$ of increasing length such that $f(p_i) = x_i$ with p_i being a minimal description of x_i under f, so that $C_f(x_i) = |p_i|$. Select a subsequence $q_1, q_2, \cdots$ from $p_1, p_2, \cdots$ such that for every $i \ge 1$, $|q_i| > 2|p_i|$. Now define a description method $g : \Sigma^* \to \Sigma^*$ as follows: $g(p_j) = f(q_j)$ for each $j \ge 1$, and g coincides with f everywhere else. Now, for each $y_j = f(q_j)$ for $j \ge 1$, we have

$$C_g(y_j) \le |p_j| < |q_j|/2 = C_f(y_j)/2 \ .$$

We conclude that for infinitely many strings z, $C_g(z) < C_f(z)/2$, and thus f does not minorize g. Therefore no single f can minorize every other partial function.

We will now restrict the class of descriptions in a meaningful way so that a best description method will emerge. Note that for a description to be useful, it also seems reasonable to require that there be an effective, computable procedure to compute the object. In other words, we impose that

[1] Note that such a minimal U need not be unique, since it is possible for two functions can minorize each other. But this causes no harm since any such minimal method would do equally well for our theory.

the description method f be a partial recursive function (which is the concept analogous to Turing-recognizability for functions). That is, there must be a Turing machine which on input p such that $f(p) = x$, halts with x as output on the tape. Under this restriction on description methods, we argue below that the class of partial recursive functions has a minimal description method say U, namely the one corresponding to the Universal Turing Machine (UTM) that minorizes every other partial recursive function. Define $U(\langle M, w\rangle)$ to be the output of Turing machine M on input w; U is the partial recursive function computed by the UTM. Then clearly

$$C_U(x) = \min\{|\langle M, w\rangle| \ : \ \text{TM } M \text{ on input } w \text{ halts with output } x\} \tag{2}$$

We now show U minorizes description using any other Turing machine U'. Let x be arbitrary, and let p be a shortest description of x under U', so that $U'(p) = x$, i.e. U' outputs x on input p. Now clearly the output of the UTM U on input $\langle U', p\rangle$ equals x, and thus $U(\langle U', p\rangle) = x$. Hence

$$C_U(x) \leq |\langle U', p\rangle| = c_{U'} + |p| = c_{U'} + C_{U'}(x)$$

where $c_{U'}$ is a constant that depends only on U' (and importantly is independent of x).

We use $C_U(x)$ defined in Equation (1) as the *Kolmogorov complexity* of x, and denote it by $K(x)$ (which is the notation used in Sipser's text). In the next lecture, we will prove interesting properties about the function $K(x)$.