Exercise 19.3.2: Let $A \subseteq \mathbb{N}$ be any set. Let $\chi_A = b_0 b_1 b_2 \cdots$ be the ω-string such that $b_i = 1$ iff $i \in$. Write $\chi_A[i : j]$ for $b_i b_{i+1} \cdots b_j$, and $\chi_A[j]$ for $\chi_A[0 : j]$.
(i) For all recursive A, there exists a constant $c = c(A)$ such that $K'(\chi_A[n]) \leq c$.
(ii) For all r.e. A, there is a constant $c = c(A)$ such that $K'(\chi_A[n]) \leq \ell(n) + c$. □

End Exercise

19.4 Some Applications

Kolmogorov Complexity has many applications, typically in lower bound proofs. For instance, in showing the existence of "random" or "hard" instances in a suitable class. Such arguments amounts to a sophisticated form of counting, and are especially amenable in the Kolmogorov Complexity framework. The advantage of such a framework is often conciseness (since the basic facts of Kolmogorov Complexity can be taken as given). Having a single framework to approach a variety of problems also a source of satisfaction.

In such applications, we will be handling general objects (Turing machines, graphs, crossing sequences, etc) as arguments to our Kolmogorov Complexity function $K(x|y)$. For instance, if G is a graph we must assume some encoding of G as a number denoted $\langle G \rangle$. Instead of writing $K(\langle G \rangle)$, we will freely write $K(G)$. In general, for any kind of object X there is an implicit encoding $\langle X \rangle$. We may need to handle a seqeuence $X_1, X_2, \ldots, X_m$ of objects, and thus need an encoding $\langle X_1, \ldots, X_m \rangle$. Instead of writing $K(\langle X \rangle | \langle X_1, \ldots, X_m \rangle)$, we simply write $K(X|X_1, \ldots, X_m)$. Furthermore, we will write $\ell(X), \ell(X_1, \ldots, X_m)$ for the length of these encodings. Another notational device is to write $(X|Y)$ (read "X given Y" instead of $\langle X, Y \rangle$. This is useful for the conditioning interpretation of arguments.

19.4.1 Crossing Sequences

We revisit the crossing sequence arguments in Chapter 2, Section 10. Throughout the following discussion, let M be a nondeterministic multitape Turing machine accepting the binary palindromes, $L_{\texttt{pal}} = \{x \in \{0,1\}^* : x = x^R\}$. Let M accept in time-space (t, s). In Chapter 2, it was shown that

$$t(n)s(n) = \Omega(n^2).$$

We now give a proof based on Kolmogorov Complexity, but assuming that M is a deterministic machine.

Recall that a storage configuration C_j is like a configuration except that the input tape contents and input head position are omitted. If a configuration is $\langle q, w_i, n_i \rangle_{i=0}^k$, then the corresponding storage configuration is just $\langle q, w_i, n_i \rangle_{i=1}^k$. If π is an accepting computation path of M on an input x of length n, and $i = 0, \ldots, n$, then an **i-crossing sequence relative to** π is $S = (C_1, \ldots, C_m)$ where C_j $(j = 1, \ldots, m)$ is the storage configuration in π when the input head of M crosses from cell i to cell $i+1$ for the $(j+1)/2$-th time (assuming odd j) or from cell $i+1$ to cell i for the $(j/2)$-th time (assuming even j). Each C_j can be represented by a string of length $O(\lg |Q| + s(3n)) = O_M(s(3n))$, where Q is the state set of M. Since $|S| = m$, we have

$$\ell(S) = O(ms(n)). \tag{13}$$

We may also assume that M always returns its input head to position 0 before accepting, and this means that we only need consider crossing sequence of even length $m = |S|$.

Lemma 10 *For any y, there exists There exists x of length n such that for all $i = \lceil n/3 \rceil, \ldots, n$, $K(x_i|y) \geq n/3 - 4\ell(n)$. Here x_i is prefix of x of length i.*

Proof. By incompressibility (Theorem 6), there exists x of length n such that $K(x|\langle M, n \rangle) \geq n$. Let U be the reference machine for K. Consider a TM N which, given $(\langle w, z \rangle | y)$, outputs $U(z|y)w$. So, if z is a U-program for x_i given y, and $x_i w = x$ then $\langle w, z \rangle$ is N-program for x given y. Since $\ell(\langle w, z \rangle) \leq \ell(z) + \ell(w) + 2\ell(\ell(w)) + 1$ and $\ell(w) = n - i$, we obtain

$$K_N(x|y) \leq K(x_i|y) + (n-i) + 2\ell(n-i) + 1 \leq K(x_i|y) + n/3 + 3\ell(n)$$

provided $\ell(n) \geq 1$. By invariance,

$$n \leq K(x|y) \leq K_N(x|y) + C \leq K(x_i|y) + 2n/3 + 4\ell(n)$$

provided $\ell(n) \geq C$. Thus $K(x_i|y) \geq n/3 - 4\ell(n)$, as claimed. Note that C depends on N and K, but not on M, n, y, x. **Q.E.D.**

We give two related definitions:
(A) A sequence S of storage configurations is called an (M, i)**-sequence** if there exists an accepting computation path π of M on some x where $|x| \geq 2i$, and S is an i-crossing sequence relative to π. Furthermore, the prefix x_i of x of length $|x_i| = i$ is called a **witness** for S.
(B) If S is any sequence of storage configurations and w a word, we say (w, S) is **compatible** iff the following Turing machine N accepts (w, S). On input $(\langle w, S\rangle|\langle M\rangle)$, N will simulate M on input w "modulo S". This means that, as long as the input head of M does read past the end of w, the simulation is normal. Let $S = (C_1, \ldots, C_m)$, m even. Immediately after the jth time ($j = 1, 2, \ldots, m/2$) when M moves its input head from position $|w| = i$ to position $i + 1$, N will check to see if the current storage configuration of M is equal to C_{2j-1}. If not, N rejects. Otherwise, N replaces the current storage configuration with C_{2j}, and continues its simulation with input head at position i. After C_m has been installed in this manner, N accepts $\langle w, S\rangle$ iff M goes on to accept its input without ever crossing to cell $i + 1$ again.

Lemma 11 *Let S be an (M, i)-sequence.*
(i) There is a unique w of length i such that (w, S) is compatible.
(ii) There is a unique witness of length i for S.
(iii) If w is the witness for S then $K(w|M) \leq \ell(S) + 3\ell(|w|)$.

Proof.
(i) By definition of (M, i)-sequence, S has a witness w of length i. It is also clear that (w, S) is compatible. Next, for any w' of length i, we claim that if (w', S) is compatible then $w = w'$. To see this, note that since w is a witness, there is a palindrome v such that S is the $|w|$-crossing sequence relative to π, where π is the accepting computation of M on wvw^R, It follows from the compatibility of (w', S) that M also accepts $w'vw^R$. This means $w'vw^R$ is a palindrome and hence $w' = w$.
(ii) We know that (w, S) is compatible when w is a witness of S. From part (i), there is a unique u of length i such that (u, S) is compatible. We conclude that any witness of length i for S must be equal to this unique u.
(iii) Consider the Turing machine T that on input $(\langle i, S\rangle|\langle M\rangle)$ will generate each string w of length i in turn. For each w, T will check if (w, S) is compatible (using N above). If so, T outputs w. If not, T tests the next string of length i. It follows that $\langle |w|, S\rangle$ is a T-program for w given M. Hence

$$K_T(w|M) \leq \ell(|w|, S) \leq \ell(S) + 2\ell(|w|).$$

By invariance, $K(w|M) \leq \ell(S) + 2\ell(|w|) + C \leq \ell(S) + 3\ell(|w|)$, assuming $\ell(|w|) \geq C$, as desired. Note that C depends on T, and hence on N, but does not depend on M or w. **Q.E.D.**

Theorem 12 *For all deterministic M that accepts $L_{\texttt{pal}}$ in time-space $(t(n), s(n))$, and for all $n \in \mathbb{N}$ sufficiently large, there is a constant $C > 0$ such that $t(n)s(n) \geq Cn^2$.*

Proof. By Lemma 10, there is an x of length n such that $K(x_i|M, n) \geq n/3 - 4\ell(n)$ for all $i \geq \lceil n/3\rceil$. Let S_i be the i-crossing sequence for the accepting computation path of M on input x. By Lemma 11(iii), for $i \leq n/2$, $K(x_i|M) \leq \ell(S_i) + 3\ell(n)$. Hence $\ell(S_i) \geq n/3 - 7\ell(n)$. If the length of S_i is t_i then $\ell(S_i) = Ct_i s(n))$ where C depends on M (see (13)). Summing over all $i = \lceil n/3\rceil, \ldots, \lfloor n/2\rfloor$, we obtain

$$\begin{aligned}
t(n)s(n) &\geq \sum_{i=\lceil n/3\rceil}^{\lfloor n/2\rfloor} t_i s(n) \\
&\geq \sum_i C\ell(S_i) \\
&\geq C\sum_i \left(\frac{n}{3} - 7\ell(n)\right) \\
&= \Omega(n^2).
\end{aligned}$$

Q.E.D.