A DECISION PROBLEM FOR RANDOM NUMBER GENERATORS

David McGoveran
Alternative Technologies
15905 Bear Creek Road
Boulder Creek, California 95006

Consider a system composed of three elements: (1) a universal Turing machine, (2) a finite memory, and (3) a number generator. It will be shown that such a system is incapable of deciding whether or not the number generator produces repeating binary strings of length n whenever the memory is smaller than an amount m equal to n + log n.

For suppose that the Turing machine takes as input a particular string of length n and we wish it to determine whether or not the number generator is producing this string repeatedly. The Turing machine must consume an amount of memory equal to n in order to store the string. It can then scan the output of the number generator, comparing it to the first symbol of the target string. First, we need a counter to point successive symbols of the target string. This will require an amount of memory equal to x such that n = (2exp x). Whenever the Turing machine detects the symbol pointed to by the counter, it increments the counter and continues scanning. If it detects a symbol not equivalent to the one being pointed to, the counter is reset to point to the first symbol. If the counter reaches the end of the target string (is set to all 1's), then the full string has been detected. The counter is reset to point to the first symbol of the target string and the scanning continues.

It follows that the system can not decide whether or not the target string has been produced if it has memory less than n + log n. But this means that the system can not distinguish between number generators which produce repeating strings and random numbers. Clearly, the symbols in the repeating strings will occur with equal probability, as required for a random distribution. However, since the system can not detect that a given string is repeating, it can not detect that <u>some</u> string of length n is repeating. Thus, for system with less than n + log n memory, a generator producing repeating strings of length n is indistinguishable from a generator producting random numbers.