A Comment Regarding KT and Circuit Size

Eric Allender
Rutgers University, NJ, USA

Dieter van Melkebeek
University of Wisconsin-Madison, WI, USA

Abstract

This short note provides a clarification of the relationship between circuit size and KT complexity.

2012 ACM Subject Classification Complexity Classes; Problems, Circuit complexity.

Keywords and phrases Circuit Size, Kolmogorov Complexity

We were recently made aware of a misunderstanding concerning part 2 of Theorem 11 of [1]. An alert reader [3] pointed out that, since the empty set is accepted by a circuit of size $O(1)$, it should follow that $\mathrm{Size}(0^n) = O(1)$, whereas $\mathsf{KT}^A(0^n)$ must be at least $\lfloor \log n \rfloor$ for infinitely many n (since n can be retrieved from the description d underlying $\mathsf{KT}^A(0^n)$, at least one of the $2^{\ell-1}$ values of n of any given bitlength $\ell = \lfloor \log n \rfloor + 1$ needs to have $|d| \geq \ell - 1$). This seems to contradict the second part of Theorem 11.

The best way that we can explain this apparent contradiction, is by asserting that we had intended that the definition of "circuit size" should entail that a circuit C_n taking inputs of length n should have size at least n. Some later work dealing with KT complexity has explicitly required that the size of C_n be at least n. For example, consider [2, Lemma 2.3]; the paragraph before Lemma 2.3 describes states that it is a "convention" that an n-input circuit has "size" at least n (which is probably more accurate than to present this as a "lemma").

In [1] circuit size is defined as the number of connections, which does not preclude having circuits of size $O(1)$. A suitable definition for our purposes is the sum of the number of input gates and the number of connections. The first term guarantees that the size of C_n is at least n; the second term guarantees that the length of oracle queries made by C_n does not exceed the size of C_n.

If "size" is defined in this way, then both parts of Theorem 11 in [1] are true, although we should have considered the cases where $i > |x|$ in both parts and have described how to distinguish between those cases and the ones where $i \leq |x|$ when analyzing $\mathsf{KT}^A(x)$.

References

1 Eric Allender, Harry Buhrman, Michal Koucký, Dieter Van Melkebeek, and Detlef Ronneburger. Power from random strings. *SIAM Journal on Computing*, 35(6):1467–1493, 2006. `doi:10.1137/050628994`.

2 Eric Allender, Mahdi Cheraghchi, Dimitrios Myrisiotis, Harsha Tirumala, and Ilya Volkovich. One-way functions and a conditional variant of MKTP. In *41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, volume 213 of *LIPIcs*, pages 7:1–7:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. `doi:10.4230/LIPIcs.FSTTCS.2021.7`.

3 Alexey Milovanov. Personal communication, 2024.