MR3056060 (Review) 68Q15 03F30 68Q30
Allender, Eric (1-RTG-CNB); **Davie, George** (SA-SAFR);
Friedman, Luke (1-RTG-CNB); **Hopkins, Samuel B.** (1-WA-NDM);
Tzameret, Iddo (PRC-TSI-TCS)

Kolmogorov complexity, circuits, and the strength of formal theories of arithmetic. (English summary)

Chic. J. Theoret. Comput. Sci. **2013,** *Article* 5, 15 *pp.*

From the summary: "Can complexity classes be characterized in terms of efficient reducibility to the (undecidable) set of Kolmogorov-random strings? Although this might seem improbable, a series of papers has recently provided evidence that this may be the case. In particular, it is known that there is a class of problems $\mathcal{C}$ defined in terms of polynomial-time truth-table reducibility to RK (the set of Kolmogorov-random strings) that lies between BPP and PSPACE.

"The results in this paper were obtained, as part of an investigation of whether this upper bound can be improved, to show

$$(*) \qquad \mathrm{BPP} \subseteq \mathcal{C} \subseteq \mathrm{PSPACE} \cap \mathrm{P/poly}.$$

In fact, we conjecture that $\mathcal{C} = \mathrm{BPP} = \mathrm{P}$, and we close this paper with a discussion of the possibility this might be an avenue for trying to prove the equality of BPP and P.

"In this paper, we present a collection of true statements in the language of arithmetic, (each provable in ZF) and show that if these statements can be proved in certain extensions of Peano Arithmetic (PA), then (∗) holds. Although it was subsequently proved that infinitely many of these statements are, in fact, independent of those extensions of PA [E. W. Allender et al., in *Mathematical foundations of computer science 2012*, 88–99, Lecture Notes in Comput. Sci., 7464, Springer, Heidelberg, 2012; MR3030423], we present these results in the hope that related ideas may yet contribute to a proof of $\mathcal{C} = \mathrm{BPP}$, and because this work did serve as a springboard for subsequent work in the area [op. cit.]."

Saeed Salehi