Abstract

Synchronizing finite automaton is driving it into the designated state, no matter which state it was in before applying the sequence of actions. The concept gained significant attention amongst theoretical computer scientist, as well as it has numerous practical applications. This thesis focuses on several problems concerning synchronization of finite automata.

Section 2 introduces necessary preliminaries used in the latter sections of thesis, discusses the notion of synchronization and its generalizations as well as summarizes the most important applications of it.

We investigate the impact of the alphabet size on the length of carefully synchronizing words in Section 3. The results from that were presented at the CIAA 2022 conference in Rouen.

Section 4 is devoted to defining the class of deterministic finite automata (DFA) with coinciding cycles and proving the quadratic upper bounds for the length of the shortest synchronizing words for such automata. These results were presented at the DLT 2023 conference in Umeå.

In Section 5 we inquire into the problem of careful synchronizability of one-cluster partial finite automata (PFA). We managed to show examples of one-cluster automata having the shortest carefully synchronizing word of exponential length (all other known examples of such extremal families had more than one cluster) and proved that determining if a given one-cluster PFA is carefully synchronizing is NP-hard even for a two-letter alphabet. These results are accepted for presentation and inclusion in proceedings at the DLT 2024 conference in Göttingen.

Finally, we investigate the problem of developing a public-private key cryptosystem that grounds its security (even partially) on the problem of careful synchronization in Section 6. We describe the scheme of ciphering and deciphering, attempt to accomplish initial cryptanalysis of the system, as well as discuss the problem of defining and generating the key for encryption and decryption.