

Információátadás-nélküli bizonyítások

Kivonat

Borgula Annamária

Témavezető: Dr. Kiss Sándor

Budapesti Műszaki és Gazdaságtudományi Egyetem

A szakdolgozatom célja, hogy információátadás-nélküli bizonyítási eljárásokat mutassak be, az általános lépésektől eljutva néhány speciális példáig, főként a gráfelmélet területéről. Az általam bemutatott algoritmusok által érintett témák közül az első a varázslatos barlang, ami egy nagyon szemléletes példa, ez alapján bárki könnyedén megértheti, miről is szólnak ezen fajta bizonyítások. A másik három példa azonban mind NP-teljes probléma: két gráf közti izomorfizmus megtalálása, a gráfok három-színezhetősége, illetve Hamilton-körök keresése.

Ezen kívül nagy hangsúlyt kaptak az információátadás-nélküli személyazonosítási eljárások is. Szakdolgozatomban a sakk-nagymester problémát, a maffia-, terrorista- és több személyiség-csalásokat, az útlevelek kölcsönzésének problémáját mutatom be, valamint ezen csalások elleni fellépéseket mutatok.

Szó van továbbá két algoritmus-fejlesztési lehetőségről is, az egyik az algoritmus köreinek párhuzamosítása, a másik pedig a neminteraktív tétel.