

Polinomazonosságok tesztelése

Dornai Zsófia

Témavezető: Rónyai Lajos

Szakedolgozat kivonat

A szakdolgozatomban a polinomazonosságok tesztelésével foglalkozom. A témakör alapproblémája, ami jelenleg még egy nyitott kérdés, a következőképpen fogalmazható meg: találjunk egy determinisztikus polinom idejű algoritmust annak eldöntésére, hogy egy polinom az azonosan nulla polinom-e. Erre a feladatra jelenleg csak randomizált polinom idejű algoritmust ismerünk, ami azért is érdekes, mert felveti a kérdést, hogy a véletlen valóban ekkorát tud-e segíteni egy algoritmus hatékonyságában.

A dolgozatomban bevezető részében ismertetem az alapproblémát, hogy miért is ilyen elgondolkodtató ez a feladat. Egy polinomot ugyanis nem mindig lehet „gyorsan” kifejteni, és többféle formában is felírhatunk egymással egyenlő polinomokat, gondolhatunk például a nevezetes azonosságokra. Továbbá bevezetem az aritmetikai hálózat fogalmát, ami tulajdonképpen egy, a polinomot leíró irányított körmentes gráf, melynek a levelei egy adott test fölötti változókat, és elemeket jelölnek, míg a közbülső csúcsok, az úgy nevezett kapuk, egy-egy a testen belül értelmezett szorzást vagy összeadást. Ebben a fejezetben ismertetem a Schwarz–Zippel-lemma alapján azt a polinom idejű randomizált algoritmust is, ami talán a legfontosabb eljárás a feladat megoldására. Az algoritmus alapötlete, hogy véletlenszerűen választott pontokon kiértékelve egy polinomot, ha nem nulla eredményt is kapunk, akkor az nem az azonosan nulla polinom. A Schwarz–Zippel-lemma azt vizsgálja, hogy nem az azonosan nulla polinom esetén milyen valószínűséggel kapunk nulla értéket egy-egy kiértékelés alkalmával.

A továbbiakban arra mutatok elsősorban gráfelméleti példákat, hogy milyen feladatok vezethetők vissza a polinomazonosságok tesztelésének problémájára. Egy páros gráfban való teljes párosítás létének megállapításához például egy megfelelően definiált mátrix determinánsáról kell megállapítanunk, hogy az azonosan nulla polinom-e vagy sem. Ennek kapcsán kitérek a Valiant-tételre is, ami szerint minden polinom megkapható egy nem túl nagy méretű mátrix determinánsaként.

Végül ismertetek néhány fontosabb determinisztikus algoritmust, amelyek az alapprobléma speciális eseteivel foglalkoznak. Egy-egy ilyen algoritmusban tulajdonképpen a polinomot leíró aritmetikai hálózatot vizsgáljuk. Ha a hálózat felépítésével az algoritmus során nem foglalkozunk, hanem csak azzal, hogy bizonyos pontokon kiértékelve milyen értékeket kapunk, akkor fekete dobozos, ellenkező esetben fehér dobozos algoritmusról beszélünk. Mindkét esetre mutatok példát a szakdolgozatomban.