Véges projektív síkok keresése SAT-solverrel

Önálló projekt, szakmai gyakorlat I. dolgozat

Dankó Dorottya
Témavezető: Damásdi Gábor

2022. december 18.

1. Bevezetés

A félévi munkám fő célja az volt, hogy kombinatorikai problémákat vezessek vissza a SAT-feladatra és Python programnyelvben, SAT-solverek segítségével keressek rájuk megoldást. A választott problémakör a kétdimenziós véges projektív síkok keresése volt.

1.1. Véges projektív síkok

Adott pontoknak és egyeneseknek egy-egy halmaza, továbbá egy illeszkedési reláció, ami meghatározza, hogy melyik pont melyik egyenesre illeszkedik.

1.1. Definició. Azokat a struktúrákat nevezzük q-rendű véges projektív síknak, ahol

- az egyenesek és a pontok száma egyaránt $q^2 + q + 1$,
- bármely két egyenesnek létezik egy egyértelmű metszéspontja,
- bármely két ponthoz egyértelműen létezik egy egyenes, amely mindkettőre illeszkedik,
- minden egyenes pontosan $q + 1$ pontot tartalmaz,
- minden pontra pontosan $q + 1$ egyenes illeszkedik.

Jól ismert példa véges projektív síkra a Fano-sík, amelynek a rendje 2.

Nyitott kérdés, hogy milyen q-ra létezik q-rendű véges projektív sík. Az egyik legfontosabb eredmény a kérdésben Bruck és Ryser [1] nevéhez fűződik.

1.2. Tétel (Bruck-Ryser-tétel)**.** *Ha q egy véges projektív sík rendje és $q \equiv 1$ vagy $2 \pmod 4$, akkor q két egész szám négyzetének az összege.*

A Bruck-Ryser tételből következik, hogy nem létezik 6-rendű véges projektív sík. Ezen kívül 1991-ben Lam [2] bebizonyította számítógép segítségével, hogy 10-rendű sem létezik. E két eredményen kívül nem ismert más obstrukció.

Sok véges projektív sík ismert már. 9-nél kisebb rendűekre egyértelmű, de 9-rendűből négy, 49-rendűből pedig több százezer különböző létezik. A ma ismert projektív síkok rendje mind prímhatvány, sőt, minden prímhatványra létezik is példa. Ez motiválja a következő sejtést.

1.1. Sejtés. *Ha q egy véges projektív sík rendje, akkor q prímhatvány.*

1.2. SAT-solverek

A SAT-probléma elnevezése az angol satisfiability szóból ered. Adott egy logikai formula, kérdés, hogy létezik-e ennek olyan kiértékelése (a változóinak igaz-hamis értékadása), amire a formula értéke igaz lesz. Ez a probléma NP-teljes még akkor is, ha a logikai formula alakjára jelentős megszorításokat teszünk (például konjunktív normálforma alakjában minden klózban legfeljebb három változó szerepeljen, ezt nevezzük 3-SAT problémának).

Többféle algoritmust implementáltak már különböző programnyelvekben a SAT-problémára, ezeket SAT-solvereknek nevezzük. Pythonban a PySAT [3] könyvtárat arra a célra készítették, hogy logikai formulákkal és a SAT-problémával könnyen foglalkozhasson a felhasználó. Ebben többféle SAT-solver is rendelkezésünkre áll, a projektben a Glucose3 nevűt használtam. A solver inputja egy konjunktív normálforma, outputja egy igazságérték, továbbá, ha kiértékelhető a normálforma, akkor ad egy jó kiértékelést is.

2. A feladat megoldása

2.1. A probléma átfogalmazása

A félév során tehát olyan programokat írtam, ami adott q rendre a Glucose3 SAT-solvert használva megadja, hogy van-e q-rendű véges projektív sík és ha igen, akkor mutat rá egy példát. A véges projektív síkokat incidenciamátrix formában kerestem: az $A \in \mathbb{R}^{(q^2+q+1)\times(q^2+q+1)}$ mátrix sorai jelölik az egyeneseket, az oszlopai a pontokat, az a_{ij} mátrixelem 1 pontosan akkor, ha az j-edik pont rajta van az i-edik egyenesen, különben 0. A véges projektív sík definíciójában (1.1 Definíció) felsorolt tulajdonságok incidenciamátrix alakban átfogalmazva a következőket jelentik:

- minden egyenesre pontosan $q+1$ pont illeszkedik $\iff$ a mátrix minden sorában pontosan $q+1$ db egyes van
- minden ponthoz létezik pontosan $q+1$ egyenes, ami illeszkedik rá $\iff$ a mátrix minden oszlopában pontosan $q+1$ db egyes van
- nincs két olyan egyenes, melyeknek két metszéspontja lenne $\iff$ nincs a mátrixban 2 olyan i, j oszlop és k, l sor, amelyekre $a_{ik} = a_{il} = a_{jk} = a_{jl} = 1$.

Ezek a feltételek ekvivalensek a 1.1 Definícióban felsorolt feltételekkel, mert ha minden ponton átmegy $q+1$ db egyenes, és minden egyenesre teljesül az, hogy illeszkedik rá $q+1$ pont és nincs olyan egyenes, amellyel két közös pontja van, akkor minden egyenessel pontosan egy metszéspontja lesz. A szimmetria miatt igaz lesz ugyanez a pontokra is.

A konjunktív normálforma felépítéséhez a mátrix minden eleméhez egy változót rendeltünk és a fent felsorolt feltételeknek megfelelő normálformákból építettük fel a végső formulát, amit a SAT-solver inputjaként használtunk később. Az outputban az "igaz" változóknak megfelelő mátrixelemek tehát az 1-esek, a "hamis" változók pedig a 0 elemek. Az elkódoláshoz a pysat.card részkönyvtár CNF osztályát használtuk. A kódolásban a legnagyobb problémát az jelentette, hogy minden sorban és oszlopban pontosan $q+1$ db 1-es legyen. Ehhez a pysat.card CardEnc nevű absztrakt osztályához tartozó .equals() metódust használtuk, aminek bemeneti paraméterei

a korlát, ami jelen esetben $q+1$, és a logikai változók sorszámai, amelyek közül pontosan korlátnyi számú legyen igaz. Ez a függvény egy feltételt úgy kódol el, hogy a normálformában eddig nem szereplő, új logikai változókat is felvesz. A tapasztalatunk szerint ezeknek a változóknak a száma a korlát méretének emelésével nagyon megnő.

2.2. Szimmetriatörés

A probléma szimmetrikussága miatt többféle megszorítást is tehetünk a keresett megoldásra. Feltehető, hogy az első sor első $q+1$ eleme 1, a többi pedig 0. Az első $q+2$ oszlop alakját is meghatározhazjuk: feltehető, hogy az első soron kívül az első oszlop első q db eleme 1, a második oszlop második q db eleme 1, a harmadik oszlop harmadik q db eleme 1, stb. A $q+2$-edik oszlopra igaz, hogy minden korábbi oszlophoz van olyan sor, ahol mindkét elem 1-es (van egy metszéspontja minden korábbi oszloppal), ezért feltehető, hogy a $q+2$-edik sor második, $q+2$-edik, $2q+2$-edik, stb. elemei 1-esek, minden más 0. Az alábbi mátrixot adta vissza $q=3$ esetén a kód, ezen jól megfigyelhetők a szimmetriatörés megszorításai:

$$\begin{array}{cccccccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}$$

Ezekkel a megszorításokkal sikerült kicsit javítanunk a futásidőn a kisebb inputokra, viszont ötnél nagyobb rendű véges projektív síkra két heti futás után sem kaptunk eredményt.

2.3. Ciklikus projektív sík

Ciklikus véges projektív síkoknak nevezzük azokat, amiknek az incidenciamátrixa előáll olyan alakban, hogy az $i+1$-edik sor az i-ediknek az eggyel balra eltoltja (ami az i-edik sor első eleme volt, az az $i+1$-ediknek az utolsó eleme lesz). Ezeknek a SAT-solveres keresése egyszerűbb, mint az általános alakúaké, ugyanis itt elegendő egy sornak megfelelő számú változót felvenni, tehát itt q^2+q+1 változó lesz az általános eset $(q^2+q+1)^2$ db változója helyett. Az 1.1 Definíció feltételei jelen esetben a következőket jelentik:

- a változók közül pontosan $q+1$ legyen igaz
- ne legyen olyan k, hogy van két változópár, amik tagjai egymástól k távolságra vannak és mind igaz értéket vesznek fel

Mivel a feladat jóval kisebb, nagyobb q-ra is sikerült lefutnia a kódnak. 13-ig minden prímhatvány rendre talált ciklikus megoldást, $q=6$-ra pedig hamis értékkel tért vissza.

3. Összegzés

A félév során tehát véges projektív síkokat kerestem Python programnyelvben a Glucose3 SAT-solver segítségével. Általános alakú esetben $q = 2, 3, 4, 5$-rendű véges projektív síkokat találtam, ciklikus véges projektív síkokra beláttam, hogy nem létezik 6-rendű, és megmutattam, hogy létezik $2, 3, 4, 5, 7, 8, 9, 11, 13$-rendű.

Eddig tehát nem sikerült belátnom, hogy nem létezik általános alakú 6-rendű véges projektív sík. Erre kínál lehetőséget a latin négyzetek és véges projektív síkok közti összefüggés, melyet Bose mutatott meg 1938-ban. A tétel kimondása előtt azonban definiálunk néhány fogalmat.

3.1. Definició (Latin négyzet)**.** Legyen n pozitív egész szám. Adott n db különböző szimbólum. $n \times n$-es latin négyzetnek nevezzük azt a mátrixot, melynek minden sorában és minden oszlopában minden szimbólum pontosan egyszer szerepel.

3.2. Definició. Legyenek L_1 és L_2 $n \times n$ méretű latin négyzetek, és legyen L az a négyzet, aminek egy elemét úgy kapjuk, hogy a megfelelő pozícióban lévő L_1-beli elem mellé az L_2-beli elemet írjuk. Azt mondjuk, hogy L_1 és L_2 latin négyzetek ortogonálisak, ha mind az n^2 db lehetséges rendezett pár megjelenik L-ben.

Ezek után kimondhatjuk Bose tételét, ami megmutatja az összefüggést az ortogonális latin négyzetek és a véges projektív síkok között.

3.3. Tétel. *Akkor és csak akkor létezik n-rendű véges projektív sík, ha létezik $n - 1$ db $n \times n$ méretű, páronként ortogonális latin négyzet.*

Először Euler foglalkozott a 6×6-os ortogonális latin négyzetek kérdésével, az ő megfogalmazásában 36 tiszt problémaként ismert a feladat, a kérdés, hogy létezik-e két ortogonális 6×6-os latin négyzet. Ezt Tarry [4] válaszolta meg 1900-ban, amikor bebizonyította, hogy nincs két ilyen latin négyzet.

Folytatási lehetőség tehát SAT-solverekkel ortogonális latin négyzeteket keresve egy új bizonyítást adni arra, hogy nem létezik 6-rendű véges projektív sík.

Hivatkozások

[1] *R. Bruck* and *H. Ryser*: The Nonexistence of Certain Finite Projective Planes. Canadian Journal of Mathematics, 1(1), 88-93. (1949)

[2] *C. W. H. Lam*: The Search for a Finite Projective Plane of Order 10, The American Mathematical Monthly, 98:4, 305-318 (1991)

[3] *A. Ignatiev* and *A. Morgado* and *J. Marques-Silva*: PySAT: A Python Toolkit for Prototyping with SAT Oracles. Theory and Applications of Satisfiability Testing – SAT 2018, 428–437. (2018)

[4] *G. Tarry*: Le Probléme de 36 Officiers. Compte Rendu de l'Association Française pour l'Avancement des Sciences. Secrétariat de l'Association. 1: 122–123. (1900)