ELTE

Tématerületi Kiválósági Program

Ipar és Digitalizáció

Alkalmazásiterület-specifikus nagy megbízhatóságú informatikai megoldások

Titokmegosztás és véges geometriák

Ligeti Péter, Komputeralgebra tanszék, Informatikai Kar
Sziklai Péter, Szőnyi Tamás, Számítógéptudományi tanszék, Természettudományi Kar
Eötvös Loránd Tudományegyetem (ELTE)
ligetipeter@inf.elte.hu, {peter.sziklai, tamas.szonyi}@ttk.elte.hu

Bevezetés

- A titokmegosztó rendszerek a kriptológia egyik alapvető alkalmazási irányát képezik. Olyan módszerek összességéről van szó, melyekkel egy adott információt (titkot) úgy tudunk szétosztani a résztvevők között, hogy csak előre megadott, kitüntetett csoportjaik képesek rekonstruálni, az olyan részhalmazok, melyek "nem megengedettek", pedig nem jutnak semmilyen információhoz.
- Számtalan elméleti és gyakorlati alkalmazás ismert, összetett kriptográfiai protokollok felépítésétől kezdve pénzügyi és felhőalkalmazásokon át a szenzorhálózatokig. Attól függően, hogy milyen kitüntetett részhalmazokat akarunk engedélyezni, nagyon különböző sémákra van szükség. Ezek általában valamilyen mélyebb algebrai, geometriai vagy kombinatorikai eredményen alapulnak.
- Célunk olyan konstrukciók kidolgozása konkrét rendszerekre, amelyek számítási kapacitás vagy szükséges tárhely szempontjából optimálisak.
- Kódelmélet által motivált geometriai és kombinatorikai problémákat is vizsgálunk.

Alkalmazás és együttműködések

Alkalmazások: A kutatás célja hatékony konstrukciók fejlesztése olyan esetekre, amelyekben komplexebb hozzáférés-korlátozásra vagy érzékeny adatok szétosztására van szükség, pl. küszöb aláírások, vagy attribútum alapú titkosítási rendszerek.
Együttműködések:

- Aart Blokhuis, Technische Universiteit Eindhoven, Hollandia
- Christoph Reich, Hochschule Furtwangen University, Németország
- Takáts Marcella, MTA-ELTE Algebrai Geometriai Kutatócsoport

Publikációk

[1] M. Gyarmati and P. Ligeti, “Smallest graphs achieving the Stinson bound.” *IEEE Tr. on Information Theory*, 2020.

[2] P. Ligeti, P. Sziklai, and M. Takáts, “Generalized threshold secret sharing and finite geometry.” *Designs, Codes and Cryptography*, 2021 (megjelenés alatt).

[3] T. Szőnyi and Z. Weiner, “On the stability of Baer subplanes.” *European J. Combin.*, p. 103314, 2021.

[4] T. Szőnyi, A. Blokhuis, and R. Pellikaan, “The extended coset leader weight enumerator of a twisted cubic code.” *submitted to Designs, Codes and Cryptography*.

Problémák

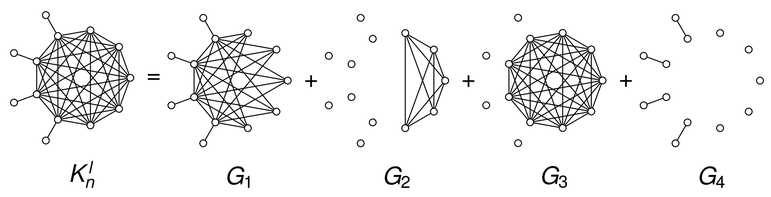
- Milyen nagyobb gráf-osztályokra lehet pontosan kiszámítani a résztvevők által tárolt információ méretét a titokhoz viszonyítva?
- Ryoh Fuji-Hara and Ying Miao eredményeiből indulva, a titokmegosztási feltételekből lineáris algebrai függetlenségi feltételeket kapunk.
- Milyen (véges test feletti) geometriai konstrukciók teljesítik a lineáris algebrai feltételeket az egyes esetekben?
- A geometriai struktúrákra (pl. lefogó ponthalmazok) milyen stabilitási eredmények vannak?
- 4 kodimenziós Reed-Solomon kódok lista dekódolásához kapcsolódó geometriai kérdések

Titokmegosztás gráfokon

- A titokmegosztás résztvevőit egy G gráf csúcsaival reprezentáljuk
- Résztvevők egy részhalmaza pontosan akkor tudja visszaállítani a titkot, ha a megfelelő csúcsok feszítenek élt
- A résztvevők által tárolt információ méretét – a Shannon entrópiákkal megadott – információs hányados méri:

$$\sigma(G) = \sup_{\mathcal{S}} \max_{v \in V(G)} \frac{\mathcal{H}(s_v)}{\mathcal{H}(s)}$$

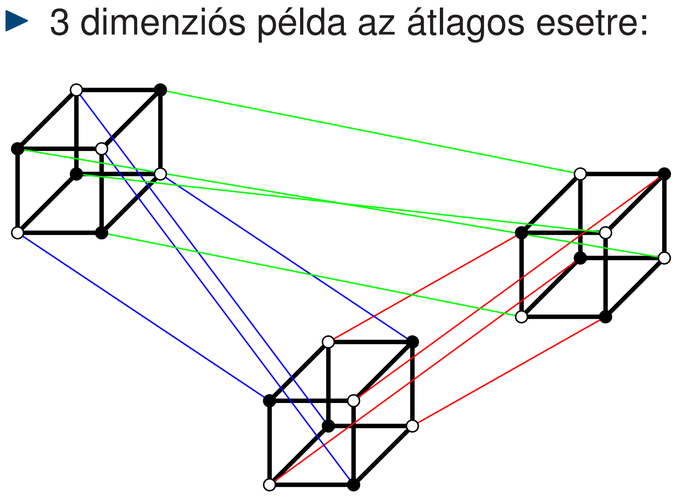
- Cél $\sigma(G)$ nem-triviális alsó és felső becsléseit megadni
- Felső korlát: konstrukciók – gráf-felbontásokkal



- Alsó korlát: entrópia módszer – LP az entrópia és a titokmegosztás tulajdonságai alapján
- A két korlát megegyezik $\Rightarrow$ pontos érték az információs hányadosra
- A hányados a maximális fokszámtól függ csak:

$$\sigma(G) = \frac{\max_{v \in V} d(v) + 1}{2}$$

- Konstrukciók aszimptotikusan legkisebb gráf osztályokra, ahol az átlagos/legrosszabb Stinson-korlát éles
- 3 dimenziós példa az átlagos esetre:



Eredmények

- Több gráfosztály ú.n. információs hányadosának pontos értékét meghatároztuk, amely a szükséges tárhely egy mérőszáma legrosszabb, illetve átlagos esetben. Sikerült megmutatni, hogy a mérőszám lényegében a maximális fokszám függvénye.
- Az ú.n. párhuzamos, ill. a hierarchikus modellre éles korlátokat bizonyítottunk a lehetséges paraméterértékekre, és további új konstrukciókat is megadtunk.
- Az úgynevezett Baer-részsíkokra, azaz az alaptest négyzetgyök rendű résztestjére épített projektív részsíkokra támaszkodó egyik konstrukció egy apró lineáris algebrai ötlettel jelentősen továbbgondolható: magasabb fokú testbővítéseket, ún. íveket és süvegeket használva a Galois geometriák elméletéből. Egy további, pici gráfos leszámlálást igénylő konstrukcióban új sémát sikerült megalkotni.
- Új, úgynevezett konjunktív multilevel sémák esetén konkrét geometriai konstrukciót adunk olyan modellre, melyben sok résztvevő van, akik (például) 3 diszjunkt csoportba sorolódnak (beosztottak, középvezetők, felsővezetők), és a titokhoz azok a részhalmazok férnek hozzá, akik legalább 4 tagúak ÉS legalább 2 vezetőt ÉS legalább 1 felsővezetőt tartalmaznak. Az alkalmazott módszerek algebraiak és geometriaiak, véges testek feletti számításokon alapulnak, pl. ún. normális racionális algebrai görbék ügyes összeépítésére épülnek.
- Stabilitási tételeket láttunk be Baer-részsíkokra (azaz ha egy lefogó ponthalmaznak kevés kitérő egyenese van és kb. annyi pontja, mint egy Baer-részsíknak, akkor kevés pont törlésével/hozzáadásával egyenest vagy Baer-részsíkot kaphatunk belőle)
- Meghatároztuk azon Reed-Solomon kód extended coset leader weight enumerator polinomját, amelynek ellenőrző mátrixa a 3-dimenziós tér normális racionális görbéje

Az Alkalmazásiterület-specifikus nagy megbízhatóságú informatikai megoldások című projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi kiválósági program (TKP2020-NKA-06, Nemzeti Kihívások Alprogram) finanszírozásában valósult meg.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

Az NKFI Alapból megvalósuló program