Czédli Gábor: 2023. április 5.

Kvázirendezés-hálók nagy főfiltereinek generálása és ezzel kapcsolatban: út a Zádori-módszertől egy titkosírásig

Egy [b) főfilter nagy, ha a (b] főideálnak kevés eleme van. Ismertetjük azt a 2023-as eredményt, amely szerint egy (nagy) A halmaz kvázirendezéseinek Quo(A) hálójában a nagy főfilterek kevés elemmel generálható (rész)hálók. Ehhez pontosan meghatározzuk, hogy mi az a legkisebb k szám, hogy az n atommal rendelkező B_n Boole-hálót (más szóval az {1,2,...,n} halmaz hatványhalmaz-hálóját) egy k-elemű részhalmaza generálja.

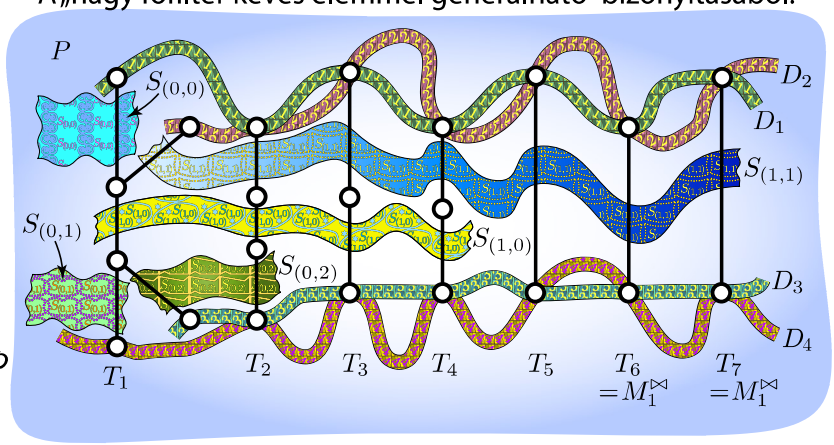
A B_n generálására vonatkozó eredmény motiválja, hogy egy 2021-es cikkben (Publ. Math. Debrecen) leírt autentikációs (és titkosírási) protokollt most a B_n Boole-hálóra alkalmazzuk. A protokoll egy NP-teljes alapproblémára épül és titkos (tehát nem nyilvános) kulcsot használ. Biztonságosnak TŰNIK - többet nem állíthatunk, hiszen egy NP-teljes problémán alapuló protokoll nagyon sebezhető is lehet (erre példát is mutatunk).

A történeti áttekintésben (a teljesség igénye nélkül és időrendben) Rudolf Wille, H. Strietz, Zádori László, Ivan Chajda, az előadó, Takách Géza, Totik Vilmos, Dolgos Tamás (Maróti Miklós tanítványa), Kulin Júlia, Lillian Oluoch és Delbrin Ahmed említendő.

Részlet [CzG - Oluoch, 2020]:

Proof of Theorem 4.4. In addition to earlier exp
particion lattices, see the References section, an id
smithing. In a traditional pin tumbler cylinder lock

A „nagy főfilter kevés elemmel generálható” bizonyításából:



További illusztráció: