MATEMATIKCENTRUM | LUNDS TEKNISKA HÖGSKOLA | PRESENTERAD 2019-05-10

EXAMENSARBETE Orthogonal decompositions of traceless matrix spaces
STUDENT Patrik Olsson
HANDLEDARE Victor Ufnarovski (LTH)
EXAMINATOR Anna Torstensson (LTH)

Vad har Nalle Puh att göra med kvantkryptering?

POPULÄRVETENSKAPLIG SAMMANFATTNING **Patrik Olsson**

Ett matematiskt problem som förblivit olöst i snart fyra decennier har betydelse för kvantkryptering.

I början av 80-talet publicerades en serie matematiska forskningsartiklar som formulerade och behandlade ett nytt problem. Frågan gällde hur långt det är möjligt att dela upp så kallade simpla liealgebror – en särskild sorts linjära rum – i ortogonala delrum. Det går att göra en jämförelse med problemet att dela upp ett vektorrum i ortogonala basvektorer, känt från linjär algebra, men istället består simpla liealgebror av matriser. Exempelvis så består en sådan klass av simpla liealgebror, kallad *klass A*, av de komplexa matriser vars spår – summan av värdena längs diagonalen – är lika med noll.

Oberoende av storleken på ett vektorrum så går det alltid att dela upp det i ortogonala basvektorer, men motsvarande gäller inte nödvändigtvis för simpla liealgebror. I de tidigare nämnda artiklarna så fanns exempelvis slutsatsen att för klassen A så går det att göra en ortogonal uppdelning om storleken på matriserna är ett primtal eller, mer generellt, en primtalspotens. Delproblemet gällande övriga storlekar visade sig å andra sidan vara oerhört komplext och ingen definitiv slutsats kunde ges mer än att det verkar troligt att ingen uppdelning finns för dessa storlekar.

Idag, nästan fyrtio år senare, är detta delproblem ännu inte helt löst. Inte ens för det första och enklaste exemplet, storlek sex, har det gått att avgöra om en ortogonal uppdelning finns eller inte. Problemet kom att kallas *Nalle Puhs problem* efter en ordvitsig dikt i den ryska översättning av A.A. Milnes klassiska bok *Nalle Puhs hörna*, som med lite fantasi kan omtolkas som en referens till problemet (A_n: storlek $n+1$ i klass A).

> Låt oss ta ordet 'igen' [ry. homofon: 'A-fem']
> Varför uttalar vi det så
> När vi lika väl kunnat säga
> 'A-sex', 'A-sju', 'A-åtta'

Med tiden så har det visat sig att det finns tillämpningar för ortogonala uppdelningar, åtminstone när det gäller för klass A liealgebror. Forskare inom kvantkryptering är intresserade av så kallade *mutually unbiased bases* och dessa är starkt kopplade till ortogonala uppdelningar. För varje mutually unbiased basis så går det att härleda en motsvarande ortogonal uppdelning, och vice versa.

Eftersom Nalle Puhs problem uppenbarligen är alltför svårt för att lösas inom ramen av ett examensarbete så har syftet istället varit att undersöka de redan kända dellösningarna av problemet från en ny vinkel. Istället för att analysera en ortogonal uppdelning direkt från dess delrum så gör jag det från hur dessa delrum är likformiga. Basbytesmatriserna för dessa likformigheter kommer ha en särskild form som är mycket enklare att arbeta med än den direkta definitionen av ortogonal uppdelning.