Integral Geometry over Finite Fields

Cataloging Inadmissibility

Includes joint work with David Feldman, and with Mehmet Orhon, both from Univ of New Hampshire (UNH)

Eric Grinberg

UMass Boston

Modern Challenges in Imaging

In the Footsteps of Allan MacLeod Cormack

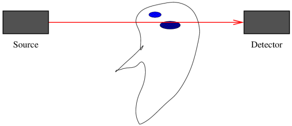
On the Fortieth Anniversary of his Nobel Prize

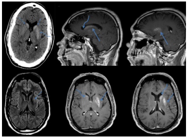
Tufts University

August 2019

Motivation: CAT Scanners and X-Ray Tomography

Crude model: CAT scanner as device that computes line integrals of density functions, using x-rays,
determines a 3-D image of the mass density of the object it scans:





Let $f(x)$ be a continuous function of compact support in $\mathbb{R}^3$.
The X-ray transform of $f(x)$, also: *the Radon transform*, is a function of lines ℓ in $\mathbb{R}^3$ called $Rf(\ell)$:

$$Rf(\ell) = \int_\ell f(x)\, d_\ell(x),$$

where $d_\ell(x)$ is the arc length measure along the line ℓ.
f can be recovered from Rf (Radon inversion).

Motivation: take fewer measurements, reduce radiation, minimal x-ray sets, still recover image

$$Rf(\ell) = \int_\ell f(x)\, d_\ell(x),$$

$$R : \{\text{point functions}\} \longrightarrow \{\text{line functions}\}$$

The set of lines in $\mathbb{R}^3$ is a Grassmann manifold. It is 4-dimensional .
(2-D for orientation of a line, 2-D for parallel translation of line along normal plane)
Since $\dim(\mathbb{R}^3) = 3$, while $\dim \left\{ \textit{lines in}\, \mathbb{R}^3 \right\} = 4$,

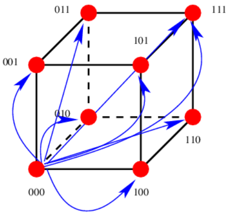
- There are "more" lines than planes
- The problem is overdetermined.
- Reasonable to expect 3-param family of lines suffices for inversion.

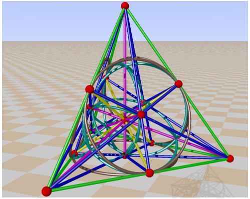
Finite models

Replace 3D space $\mathbb{R}^3$ by the 3D vector space over finite field $\mathbb{F}_2 \equiv \mathbb{Z}_2$:

$$\mathbb{F}_2^3, \text{ or its projective analog, } \mathbb{F}_q\mathbb{P}^3.$$

Replace line integrals by line sums.

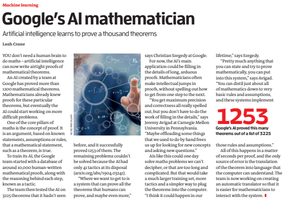




Why Finite models?

Why consider finite models?

- "All" questions can be answered in principle
- No analytic restrictions
- Possible import/export of ideas w/ continuous case
- Canonical source of interesting integral geometry questions
- Limits as $n \mapsto \infty$ may have analytic implications
- Links w/ Quantum Computing, AI auto theorem proving , Cryptography


Machine learning

Google's AI mathematician

Artificial intelligence learns to prove a thousand theorems

Leah Crane

YOU don't need a human brain to do maths – artificial intelligence can now write airtight proofs of mathematical theorems.

An AI created by a team at Google has proved more than 1200 mathematical theorems. Mathematicians already knew proofs for these particular theorems, but eventually the AI could start working on more difficult problems.

One of the core pillars of maths is the concept of proof. It is an argument, based on known statements, assumptions or rules, that a mathematical statement, such as a theorem, is true.

To train its AI, the Google team started with a database of around 10,000 human-written mathematical proofs, along with the reasoning behind each step, known as a tactic.

The team then tested the AI on 3225 theorems that it hadn't seen before, and it successfully proved 1253 of them. The remaining problems couldn't be solved because the AI had only 41 tactics at its disposal (arxiv.org/abs/1904.03241).

"Where we want to get to is a system that can prove all the theorems that humans can prove, and maybe even more," says Christian Szegedy at Google.

For now, the AI's main application could be filling in the details of long, arduous proofs. Mathematicians often make intellectual jumps in proofs, without spelling out how to get from one step to the next.

"You get maximum precision and correctness all really spelled out, but you don't have to do the work of filling in the details," says Jeremy Avigad at Carnegie Mellon University in Pennsylvania. "Maybe offloading some things that we used to do by hand frees us up for looking for new concepts and asking new questions."

AIs like this could one day solve maths problems we can't decipher, or that are too long and complicated. But that would take a much larger training set, more tactics and a simpler way to plug the theorems into the computer. "I think it could happen in our lifetime," says Szegedy.

"Pretty much anything that you can state and try to prove mathematically, you can put into this system," says Avigad. "You can distil just about all of mathematics down to very basic rules and assumptions, and these systems implement those rules and assumptions."

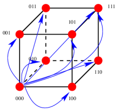
All of this happens in a matter of seconds per proof, and the only source of error is the translation of the theorem into language that the computer can understand. The team is now working on creating an automatic translator so that it is easier for mathematicians to interact with the system.

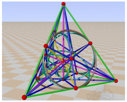
1253

Google's AI proved this many theorems out of a list of 3225

NICOEL NINO/ALAMY

About the models





The three dimensional vector space $\mathbb{F}_2^3$ has:

- 8 points
- 2 points per line
- 7 lines through a given point
- 28 lines in all

The three dimensional projective space $\mathbb{F}_2\mathbb{P}^3$ has:

- 15 points
- 3 points per line
- 7 lines through a given point
- 35 lines in all

Overdeterminacy and Line Complexes

X-Ray transform on $\mathbb{F}_2^3$ overdetermined by $28 - 8 = 20$ dimensions.
X-Ray transform on $\mathbb{F}_2\mathbb{P}^3$ overdetermined by $35 - 15 = 20$ dimensions.

Definition: a *line complex* is, in a given geometry:

> a collection of as many lines as there are points

- In $\mathbb{F}_2^3$ there are $\binom{28}{8} = 3,108,105$ line complexes
- In $\mathbb{F}_2\mathbb{P}^3$ there are $\binom{35}{15} = 3,247,943,160$ line complexes

Line complex $\mathcal{C}$ is *admissible* if:

> X-Ray transform (sums point functions) along the lines in $\mathcal{C}$ is injective.

This follows I.M.Gel'fand *admissibility* in the continuous category.

Preview:

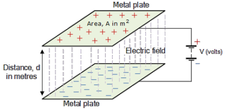
- $937,440 = 30.16$ percent $\mathbb{F}_2^3$ complexes are admissible.
- $1,238,376,132 = 38.13$ percent $\mathbb{P}\mathbb{F}_2^3$ complexes are admissible.

Admissibility for Hyperplanes–uniformity

Theorem (G.– way back)

Let $\mathcal{C}$ be a complex of hyperplanes in a vector space over a finite field. Then $\mathcal{C}$ is admissible if and only if:

- *$\mathcal{C}$ contains one entire family of parallel hyperplanes (a spread).*
- *$\mathcal{C}$ omits precisely one hyperplane from every other parallel family of spreads.*



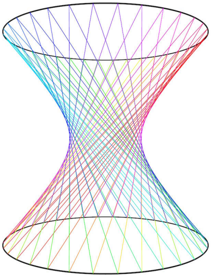
The proof is immediate:

- The full hyperplane transform is invertible by a celebrated general result of E.D. Bolker.
- If a complex of hyperplanes omits two parallel hyperplanes then a *dipole distribution* for the capacitor formed by these two hyperplanes is a *phantom*.
- If a complex of hyperplanes contains one full parallel family of hyperplanes (a *spread*) and omits at most one hyperplane from every other spread, then Radon transform data on this complex extends uniquely to the full family of hyperplanes.

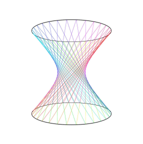
Projective space: Doubly Ruled Surfaces

Theorem (Feldman-G.)

Let $\mathcal{C}$ be a line complex in the projective space $\mathbb{P}^3$ over any finite field. Then $\mathcal{C}$ is inadmissible if and only if it contains a doubly ruled surface of lines.



Which line complexes are admissible?

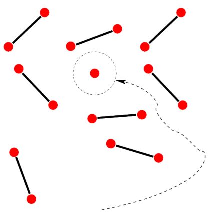


We tell our students that mathematics is value free.

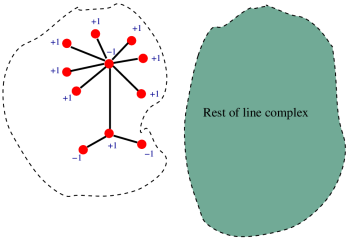
Nonetheless, we will treat admissible complexes as “good” and inadmissibles as “bad”.

“Bad” examples;

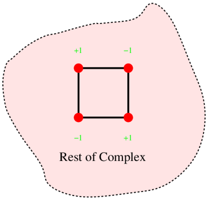
- Omitted Points
- Isolated Trees
- Even Cycles



Omitted Point



An isolated tree



A complex with an even cycle

Admissibility Theorem for $\mathbb{F}_2^3$

Theorem (G-Y2K)

A line $\mathcal{C}$ in $\mathbb{F}_2^3$ is admissible iff it omits no point and contains no even cycles nor isolated trees.

The Theorem proves itself.

Proof. It is evident that any one of the "bad" properties makes a complex inadmissible. On the other hand, assume $\mathcal{C}$ has none of the "bad' above. To determine the function value $f(p)$ at a point $p \in \mathbb{F}_2^3$, note that

- p belongs to a maximal subgraph G which is not a tree.
- This subgraph contains an odd cycle T; odd cycles are "self-invertible".
- Values of f are determined on T.
- Take a path π in G from p to T.
- Work backwards along π, determining values of f on each vertex of each line of π , until p is reached. □

Linear Operator and Brute Force Admissibles Count

The X-Ray transform on $\mathbb{F}_2^3$ is modeled by the 28×8 matrix below.
Bolker's Theorem implies that this matrix is of maximal rank.
Admissible complexes in $\mathbb{F}_2^3$ correspond to nonsingular 8×8 sumatrices.
These can be counted by a *brute force* program.

$$
\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix}
$$

A brute force program to list all admissible complexes:
There are $\binom{28}{8} = 3,108,105$ complexes in $\mathbb{Z}_2^3$.
How many are admissible?

```
a=0
mat= zeros( 28,8)
acc =0
for i=1:7
 for j=i+1:8
  acc=acc+1 ;
  mat(acc,i)=1 ;
  mat(acc,j)=1 ;
 endfor
endfor

for a1=1:21
 for a2=a1+1:22
  for a3=a2+1:23
   for a4=a3+1:24
    for a5=a4+1:25
     for a6=a5+1:26
      for a7=a6+1:27
       for a8=a7+1:28
        minor=zeros(8,8);
        minor(1,1:8) = mat(a1,1:8);
        minor(2,1:8) = mat(a2,1:8);
        minor(3,1:8) = mat(a3,1:8);
        minor(4,1:8) = mat(a4,1:8);
        minor(5,1:8) = mat(a5,1:8);
        minor(6,1:8) = mat(a6,1:8);
        minor(7,1:8) = mat(a7,1:8);
        minor(8,1:8) = mat(a8,1:8);

        a = det(minor)

        if a != 0
 printf("%d,%d,%d,%d,%d,%d,%d,%d",a1,a2,a3,a4,a5,a6,a7,a8)
        endif

       endfor
      endfor
     endfor
    endfor
   endfor
  endfor
 endfor
endfor
```

Computational and Experimental Results

First run:	937,438	admissible complexes
Second run:	937,440	admissible complexes

Suspicious
(especially since $937438 = 2 \cdot (\text{ large prime })$ $= 2\ (468{,}719)$.

On the other hand, $937440 = (2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 3 \times 5 \times 7 \times 31)$.

Better work it out by hand....

Joint work with Mehmet Orhon follows–two can count better than one.

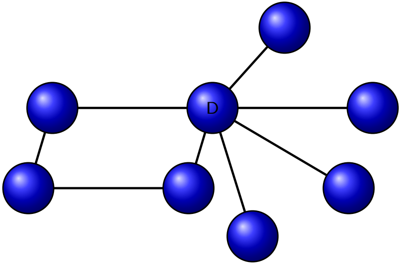
- Complexes that omit one or more points
  - Complexes that omit one point
  - Complexes that omit two or more points
  - Complexes that omit three or more points
- Additional steps . . .

Lemma

The number of connected proper line complexes with a unique 4-cycle with precisely one of its vertices of valence greater than 2 is

$$\binom{4}{1}\left[\binom{4}{4}+\binom{4}{3}\cdot 3+\binom{4}{2}\left(\binom{5}{2}-2\right)+\binom{4}{1}\left(\binom{6}{3}-4\right)\right]=500.$$

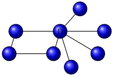
Proof. We parse the inner summands of (. . . 500) above from left to right. Choose a 4-cycle as before and mark one vertex D to have valence greater than 2.



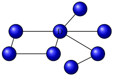
Lemma. *The number of connected proper line complexes with a unique 4-cycle with precisely one of its vertices of valence greater than 2 is*

$$\binom{4}{1}\left[\binom{4}{4}+\binom{4}{3}\cdot 3+\binom{4}{2}\left(\binom{5}{2}-2\right)+\binom{4}{1}\left(\binom{6}{3}-4\right)\right]=500.$$

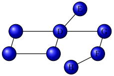
Proof. We parse the inner summands of () above from left to right. Choose a 4-cycle as before and mark one vertex D to have valence greater than 2.



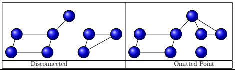
If vertex D has valence 6, there is only $1=\binom{4}{4}$ way for all 4 of the remaining points to be connected to D.



If D has valence 5, choose 3 of the 4 remaining points to be connected to D, and then choose one of these 3 to connect to the last remaining point.



If D has valence 4, choose 2 of the remaining 4 points, E, G, to connect to D. Call the remaining two points F, H. We must choose 2 lines from the 6 in the complete graph on $EFGH$. But EG is forbidden (else an isolated tree or an omitted point results), so only 2 of 5 lines are available, and we cannot choose both to go through F and omit H nor both to go through H and omit F, so we have $\binom{5}{2}-2=8$ choices. Hence there are $\binom{4}{2}\cdot\left(\binom{5}{2}-2\right)=48$ complexes with D of valence 4.



If D has valence 3, choose 1 of the remaining 4 points and connect it to the 4-cycle at D. We need to select three more lines involving the non-4-cycle points, and we must avoid forming a 3-cycle which would be a connected component, contradicting the hypothesis, or else leave one point omitted. There are 4 ways to generate a 3-cycle among the 4 remaining points, so there are $\binom{4}{1}\left(\binom{6}{3}-4\right)=4\cdot 16=64$ complexes here. $\square$

Complexes w. isolated trees, omitting no points

Lemma

The number of complexes that omit no point and contain at least one isolated line is

$$\binom{8}{2}\left[\binom{15}{7}-\binom{6}{1}\binom{10}{7}-\frac{1}{2}\binom{6}{2}\binom{6}{6}\right]=159,810$$

These complexes are counted without multiplicity.

Corollary

The number of complexes that contain isolated trees and omit no points is 200, 970. These complexes are counted without multiplicity.

Proper Complexes Containing a 4-Cycle– the most fun

- If a proper line complex has more than one 4-cycle, then the cycles must be disjoint.
- The number of proper line complexes containing more than one 4-cycle is $\binom{8}{4}\left(\frac{4!}{4\cdot 2}\right)\left(\frac{4!}{4\cdot 2}\right)\left(\frac{1}{2}\right)=315$.
- The number of topologically disconnected proper line complexes with a unique 4-cycle is: $\binom{8}{4}\left(\frac{4!}{4\cdot 2}\right)\binom{4}{1}\binom{7}{1}=5,880$.
- The number of proper line complexes with a unique 4-cycle with one of its vertices of valence greater than 2 is $\binom{4}{1}\left[\binom{4}{4}+\binom{4}{3}\cdot 3+\binom{4}{2}\left(\binom{5}{2}-2\right)+\binom{4}{1}\left(\binom{6}{3}-4\right)\right]=500$.
- The number of proper line complexes with a unique 4-cycle with 2 vertices of valence greater than 2 is: 1092.
- The number of proper line complexes with a unique 4-cycle with 3 vertices of valence greater than 2 is: 432.
- The number of proper line complexes with a unique 4-cycle with 4 points of valence greater than 2 is $4! = 24$.

Admissible Complexes: a complete count

The grand total is:

$$1456875 - (210 \cdot (24 + 432 + 1092 + 500) + 5880 + 315 + 80640 + 2520) = 937440.$$

Note that the 210 multiplier accounts for the number of ways to choose a 4-cycle among 8 points for lemmas above assuming a fixed 4-cycle has been chosen.

(There are $\binom{8}{4} = 70$ ways to choose 4 points out of 8, and $\frac{4!}{4 \cdot 2} = 3$ ways to form an unoriented 4-cycle out of 4 points; oh, and $70 \cdot 3 = 210$.)

Some references

A Scrapbook of Inadmissible Line Complexes For the X-ray Transform
Eric L. Grinberg, Mehmet Orhon
`arXiv:1907.00280 [math.CO]`

Admissible Complexes for the Projective X-Ray Transform over a Finite Field
David V. Feldman, Eric L. Grinberg
`arXiv:1707.06695 [math.MG]`

The admissibility theorem for the spatial X-ray transform over the two element field
Eric L. Grinberg
`arXiv:1907.04200 [math.CO]`
(Appeared in The Mathematical Legacy of Leon Ehrenpreis, Springer, 2012)