SAND2010-7480C

From Sylvester-Gallai Configurations to Rank Bounds: Improved Black-box Identity Test for Depth-3 Circuits

C. Seshadhri (Sandia National Labs, Livermore)
(Work done in IBM Almaden)

Joint work with
Nitin Saxena (Hausdorff Center for Mathematics)

The problem of PIT

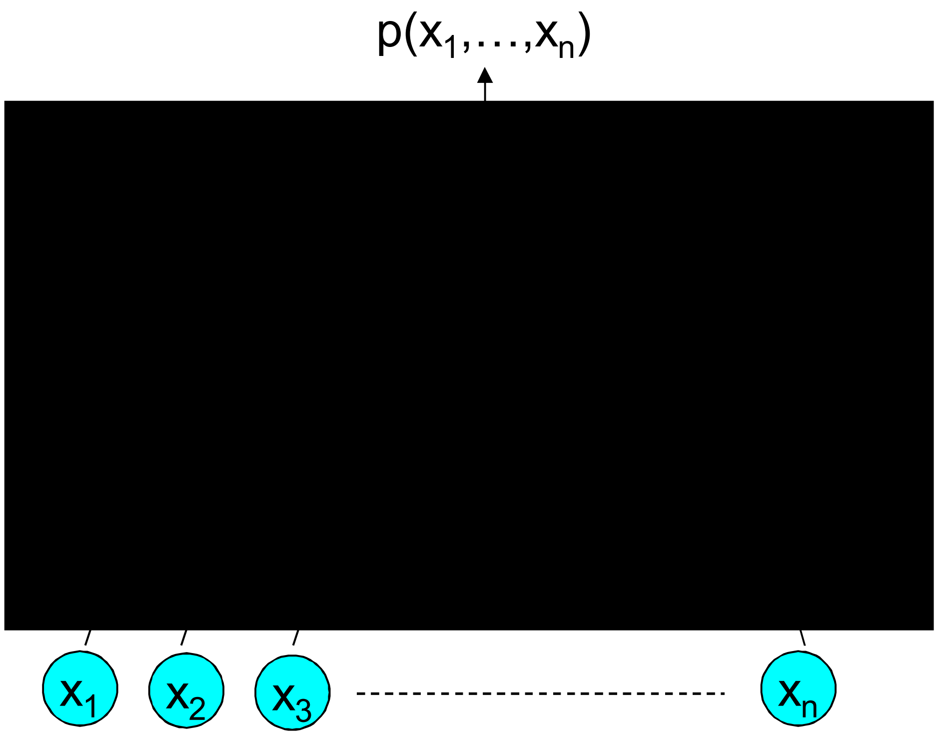
- Polynomial identity testing: given a polynomial $p(x_1,x_2,\ldots,x_n)$ over F, is it identically zero?
  - *All* coefficients of $p(x_1,\ldots,x_n)$ are zero.
  - $(x+y)^2 - x^2 - y^2 - 2xy$ is identically zero.
  - So is: $(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)$

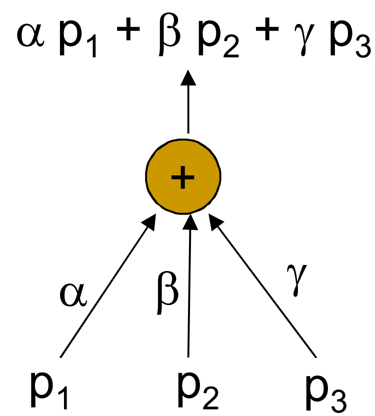
$- (aA+bB+cC+dD)^2 - (aB-bA+cD-dC)^2$

$- (aC-bD-cA+dB)^2 - (aD-dA+bC-cB)^2$

  - $x(x-1)$ is NOT identically zero over F_2.

Circuits: Blackbox or not





We want algorithm whose running time is polynomial in size of the circuit (that includes # var, degree)

- Non blackbox: can analyze structure of C
- Blackbox: cannot C
  - Feed values and see what you get

A simple, randomized test

If output is 0, we guess it is identity.

Otherwise, we know it isn't.

- [Schwartz80, Zippel79] This is a randomized blackbox poly-time algorithm.

- Big big open problem: Find a deterministic polynomial time algorithm.
  - We would really like a black box algorithm
  - Base field Q is of special interest

Why?

- Come on, it's an interesting mathematical problem. Do you need a reason?
- [Impagliazzo Kabanets 04] Derandomization implies circuit lower bounds

- [AKS] $(x + a)^n = x^n + a \pmod{n}$
- [L, MVV] Bipartite matching in NC?...
- Many more

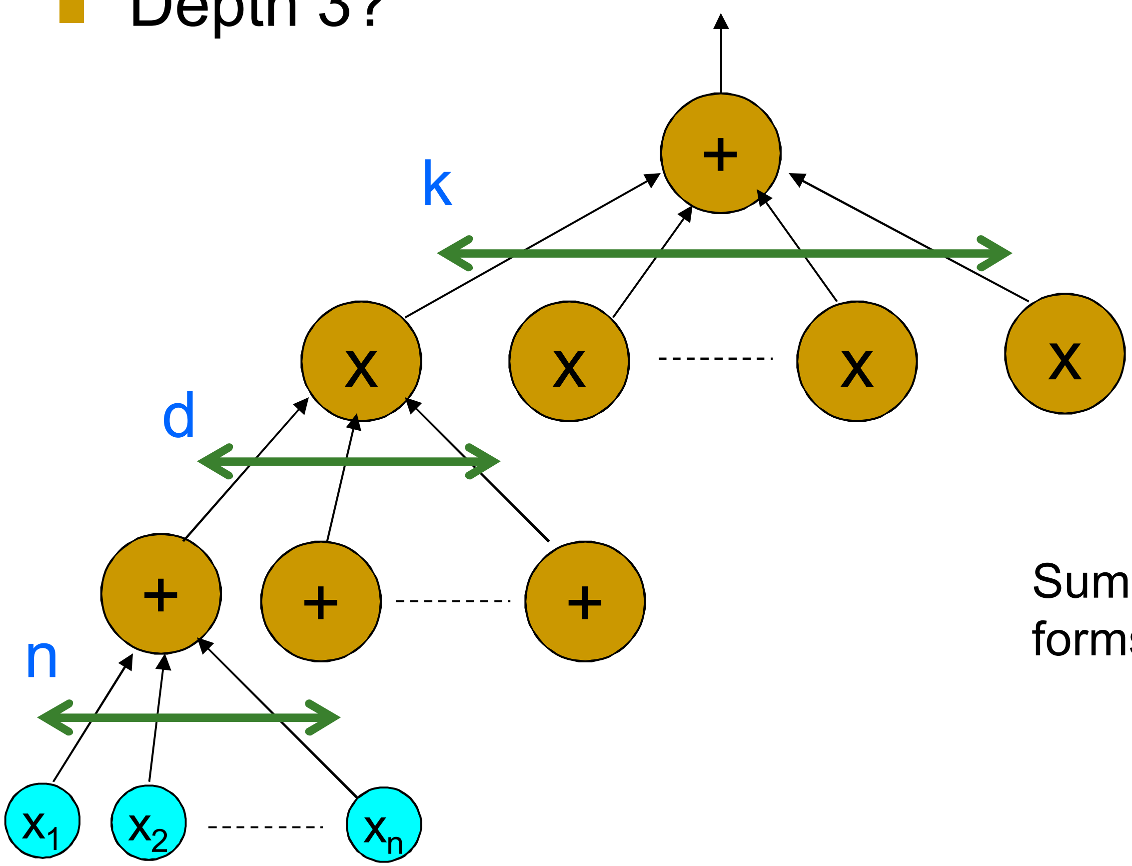
What do we do?

George Polya

If you can't solve a problem, then there is an easier problem you *can* solve. Find it.

Get shallow results

- Let's restrict the depth and see what we get
- Depth 2? Non-blackbox trivial!
  - [GK, BOT,…,KS] Polytime with blackbox
- Depth 3?



$$C = \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij} = \sum_{i=1}^{k} T_i$$

Sum of products of kd linear forms in n variables

Some examples

- Over Q

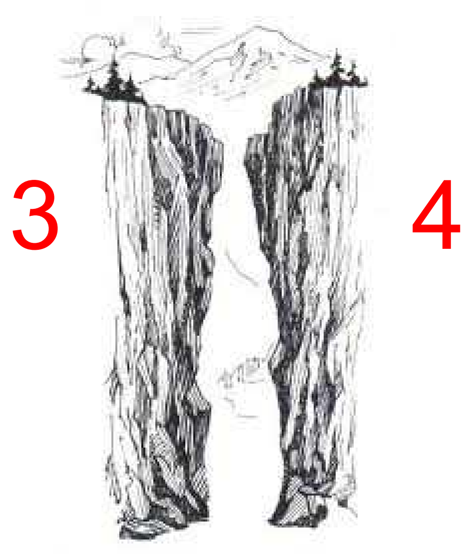
$$(x+z)(y+z) - xy - z(x+y+z) = 0$$

$$x_1x_2x_3(2y + x_1 + x_2 + x_3) - (y + x_1)(y + x_2)(y + x_3)(y + x_1 + x_2 + x_3)$$
$$+y(y + x_1 + x_2)(y + x_2 + x_3)(y + x_1 + x_3) = 0$$

- Over F_2

$$\prod_{\sum_i b_i = 0} (b_1x_1 + b_2x_2 + b_3x_3) + \prod_{\sum_i b_i = 1} (y + b_1x_1 + b_2x_2 + b_3x_3)$$
$$+ \prod_{\sum_i b_i = 0} (y + b_1x_1 + b_2x_2 + b_3x_3) = 0$$

Some good news



- [Agrawal Vinay 08] Chasm at Depth 4!
- If you can solve blackbox PIT for depth 4, then you've solved it for all depths.

- Ok, maybe it's bad news, but we have our excuse…

Our results

- So what's the best black-box running time?
  - Parameters n, d, k (think of k as constant)

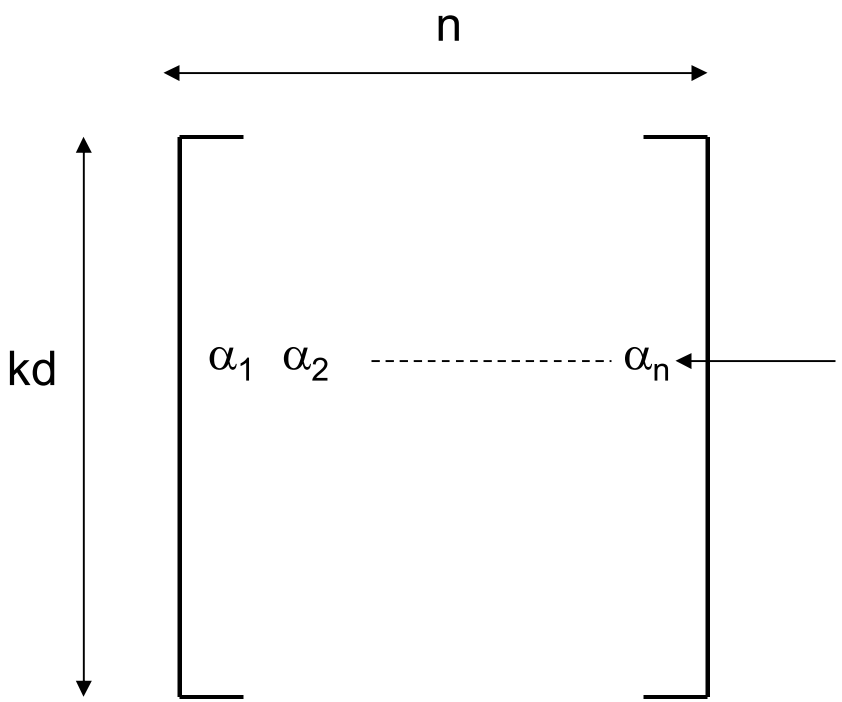
$$C \equiv \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij}$$

Who	What
[Karnin Shpilka 08] [Dvir Shpilka 06]	$\mathrm{poly}(n) d^{(\log d)^k}$
[Saxena S 09]	$\mathrm{poly}(n) d^{k^3 (\log d)}$
[Kayal Saraf 09]	$\mathrm{poly}(n) d^{k^k}$
This paper	$\mathrm{poly}(n) d^{k^2}$

- Almost matches non-blackbox test of $\mathrm{poly}(n) d^k$

The rank

M =



$$C \equiv \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij}$$

$$L_{ij} = \sum_{r=1}^{n} \alpha_r x_r$$

n-dim vector over F

Rank(C) = Rank (M)

- Introduced by [DS]: fundamental property of depth 3 circuits
- How many independent variables can an identity have?
  - An identity is very constrained, so few degrees of freedom
- [KS] Blackbox test of time poly(n)d^rank
- [DS] Rank of simple, minimal identity < $(\log d)^{k-2}$ (compare with kd)

Some examples

- Behold!

$$(x + 2y + 2z + 3w)(2x + 2y + z + 2w) - (x + y + z + w)(2x + y)$$
$$-(y + z + 2w)(3x + 3y + 2z + 3w) = 0$$

- A linear transformation tells us

$$X = x + y + z + w \qquad Y = y + z + 2w \qquad Z = 2x + y$$

- Not so impressed, are you?

$$(X + Z)(Y + Z) - XY - Z(X + Y + Z) = 0$$

What we did

- [DS 06] What is the rank of depth-3 identity (k,d,n)?
  - “We think that it is poly(k).”

- [Us] Yes, the rank is O(k^2)

- [Kayal Saraf] Rank is at most k^k

- Lower bound of rank k
- Over finite fields, rank can be (k log d)
  - We also show general bound of k^2log d

What we did

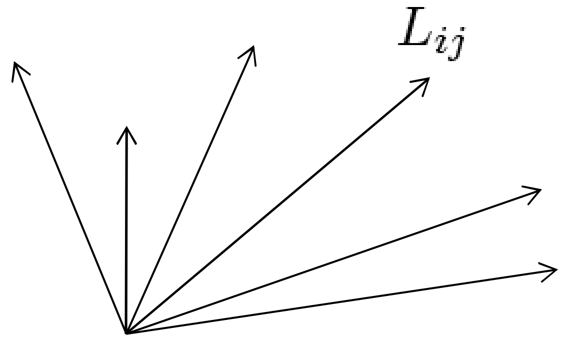
- [Kayal Saraf] Connections to Sylvester-Gallai type theorems

- We nail down this connection for all fields
  - Tighter bounds for rank

- “Building the theory of depth-3”
  - Matching structures in identities

The vector picture

$$C \equiv \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij}$$



$$L_{ij} = \sum_{r=1}^{n} \alpha_r x_r$$

n-dim vector over Q

- Totally kd vectors
- But lots of linear dependencies between them, so rank is much smaller

What dependencies?

- $C = T_1 + T_2 + T_3 = \Pi L_i + \Pi M_j + \Pi N_k = 0$
- [AB,AKS,KS] Go modulo!

$$\prod L_i + \prod M_j + \prod N_k = 0$$

Vanishes! ⟶

$$\boxed{\prod L_i} + \prod M_j + \prod N_k = 0 \pmod{L_1}$$

$$\prod M_j = -\prod N_k \pmod{L_1}$$

- By unique factorization, there is 1-1 mapping between M's and N's (they are same upto constants)

$$M_j \equiv \alpha N_k \pmod{L_i}$$

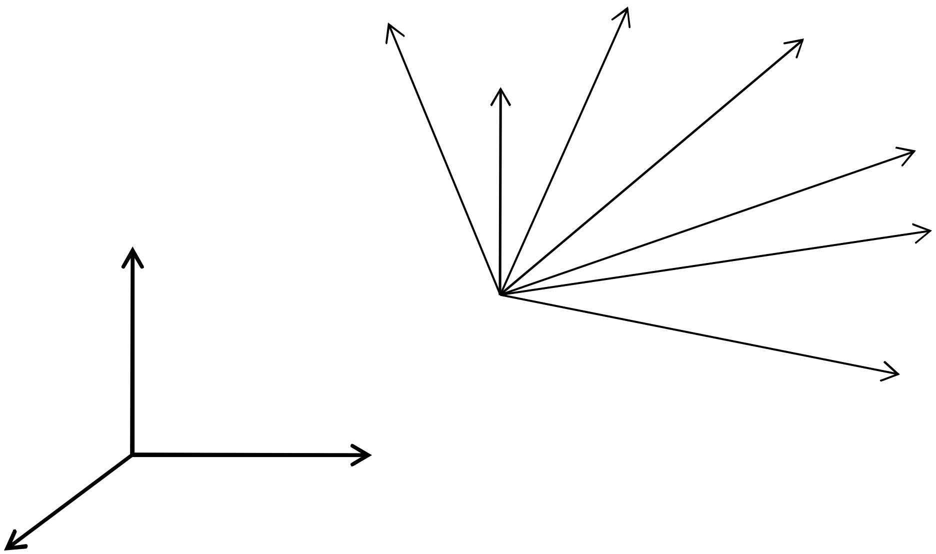
$$M_j = \alpha N_k + \beta L_i$$ (Linear dependency. Yay!)

"Mathematical question 11851", *Educational Times, 1893*

J. J. Sylvester

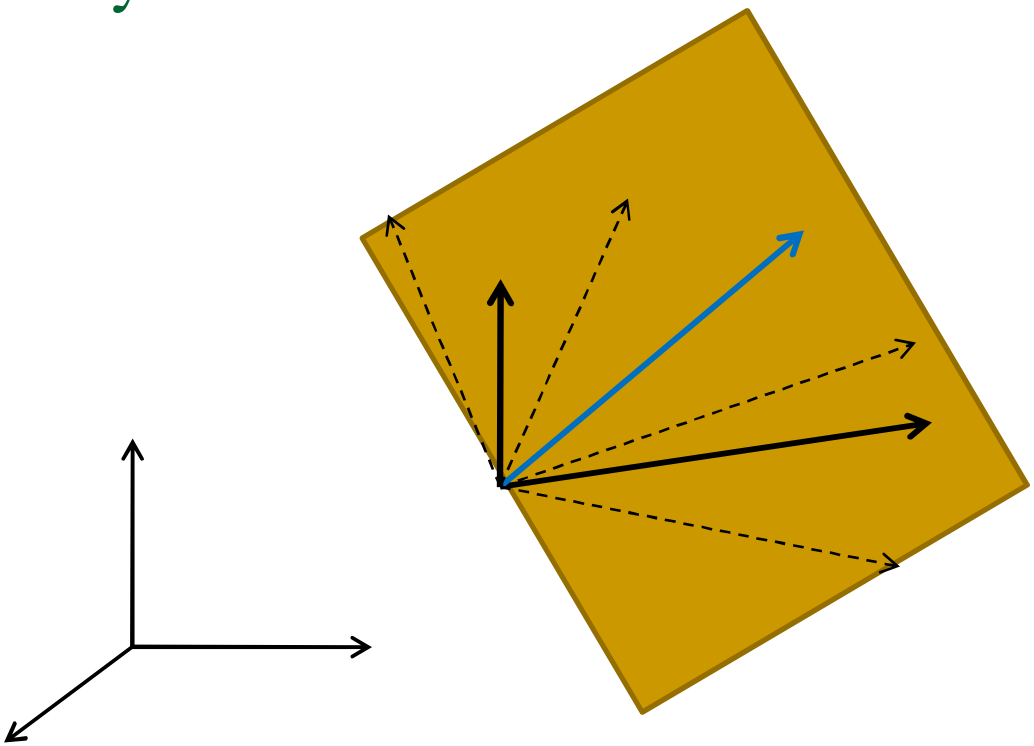
Prove that it is not possible to arrange any finite number of real points so that a right line through every two of them shall pass through a third, unless they all lie in the same right line.

Sylvester and Gallai



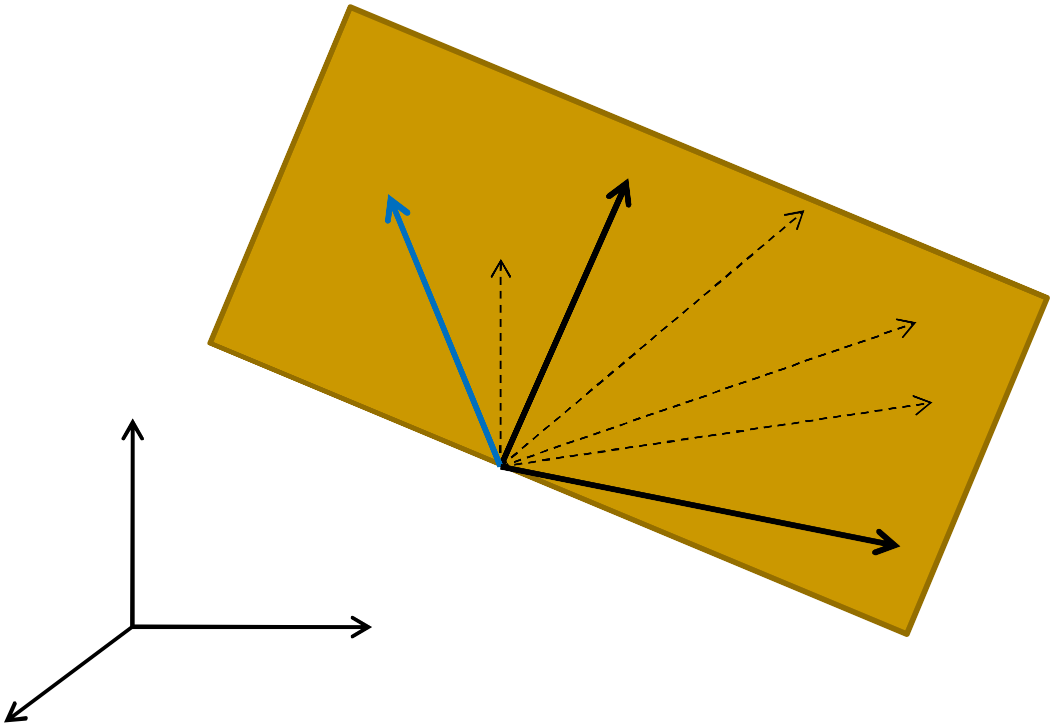
- Set of distinct vectors
- For every pair v1, v2, some v3 is in span

Sylvester and Gallai



- Set of distinct vectors
- For every pair v1, v2, some v3 is in span
- Set S is SG_2-closed

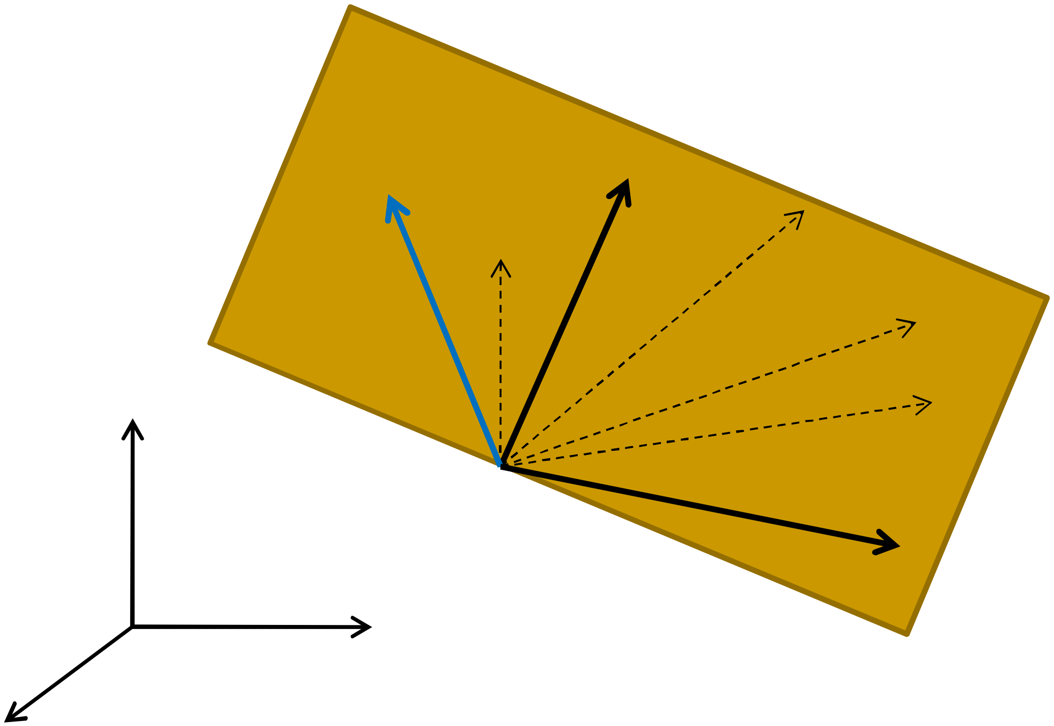
Sylvester and Gallai



- Set of distinct vectors
- For every pair v1, v2, some v3 is in span

- Set S is SG_2-closed

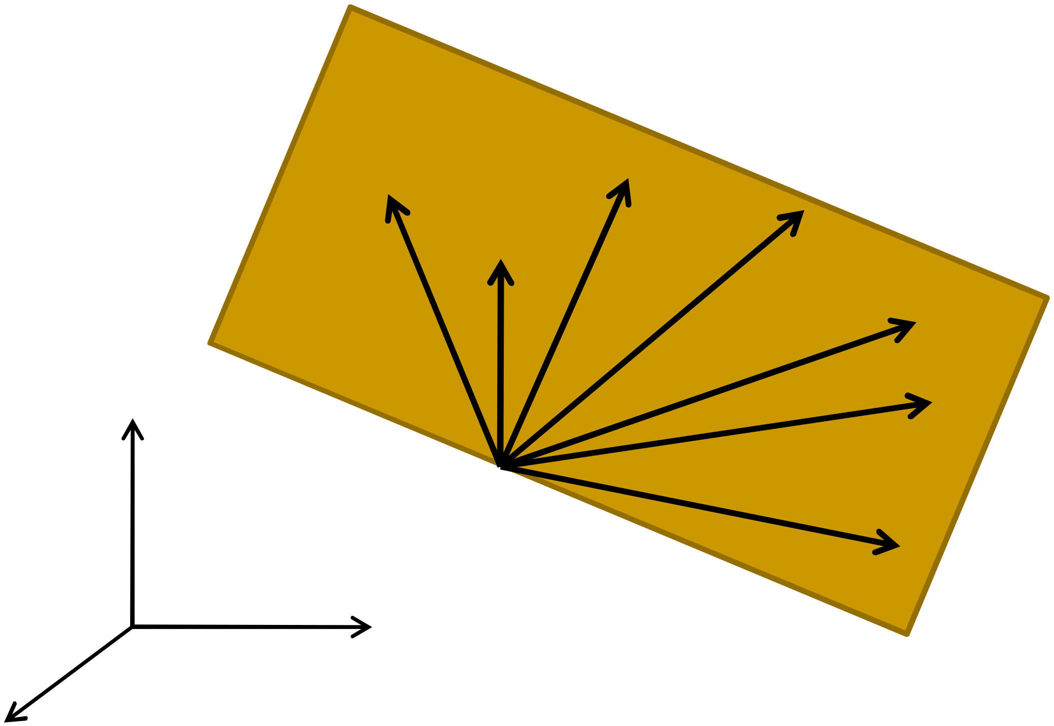
Sylvester and Gallai



- Set of distinct vectors
- For every pair v1, v2, some v3 is in span

- Set S is SG_2-closed
- [Sylvester-Gallai] Rank of SG_2-closed set over reals is at most 2!

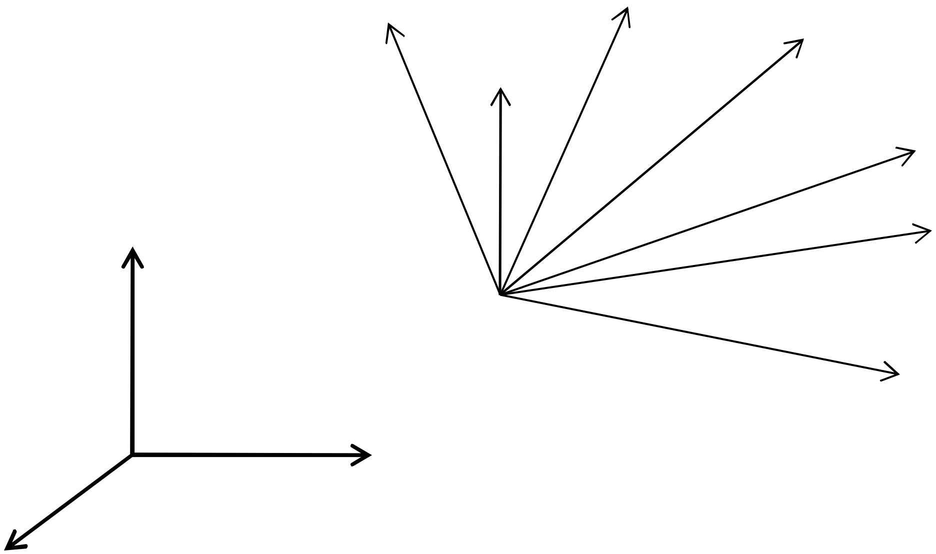
Sylvester and Gallai



- Set of distinct vectors
- For every pair v1, v2, some v3 is in span

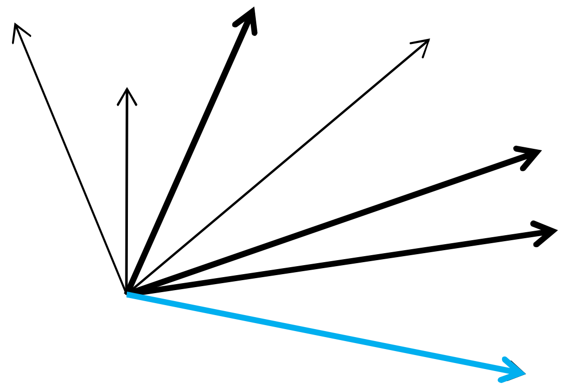
- Set S is SG_2-closed
- [Sylvester-Gallai] Rank of SG_2-closed set over reals is at most 2!
  - All vectors coplanar

Higher dimensions



- Set of distinct vectors
- For every v1, v2, v3 some v4 is in span

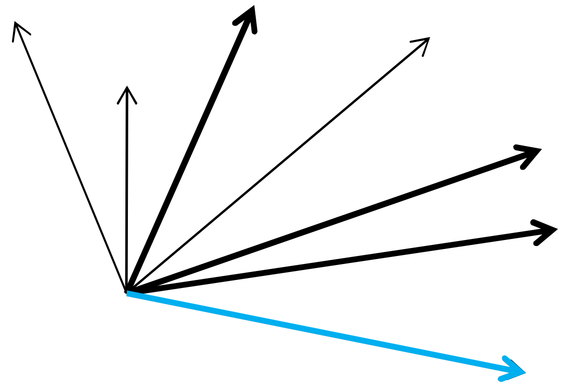
Higher dimensions



- Set of distinct vectors
- For every v1, v2, v3 some v4 is in span

- This set is SG_3-closed
- If every subset of k vectors has another vector in span, S is SG_k-closed
- Can SG_k-closed sets have high rank?

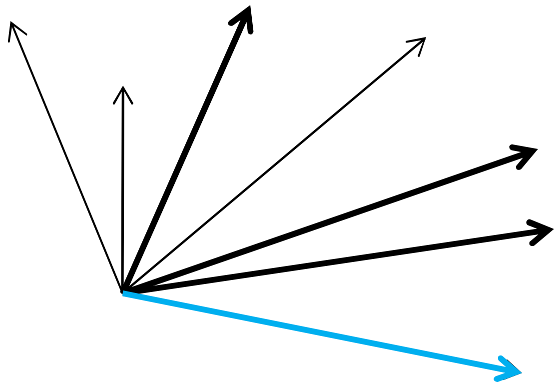
Higher dimensions



- Set of distinct vectors
- For every v1, v2, v3 some v4 is in span

- [Hansen] The rank of an SG_k-closed set < 2k-1
- Given set of m vectors over F that is SG_k-closed, what is largest possible rank?
- Sylvester-Gallai rank bound: SG_k(F,m)
  - Rank of any such set < SG_k(F,m)

Higher dimensions



- Set of distinct vectors
- For every v1, v2, v3 some v4 is in span

- [SG] SG_2(R,m) < 3
- [Hansen] SG_k(R,m) < 2k-1

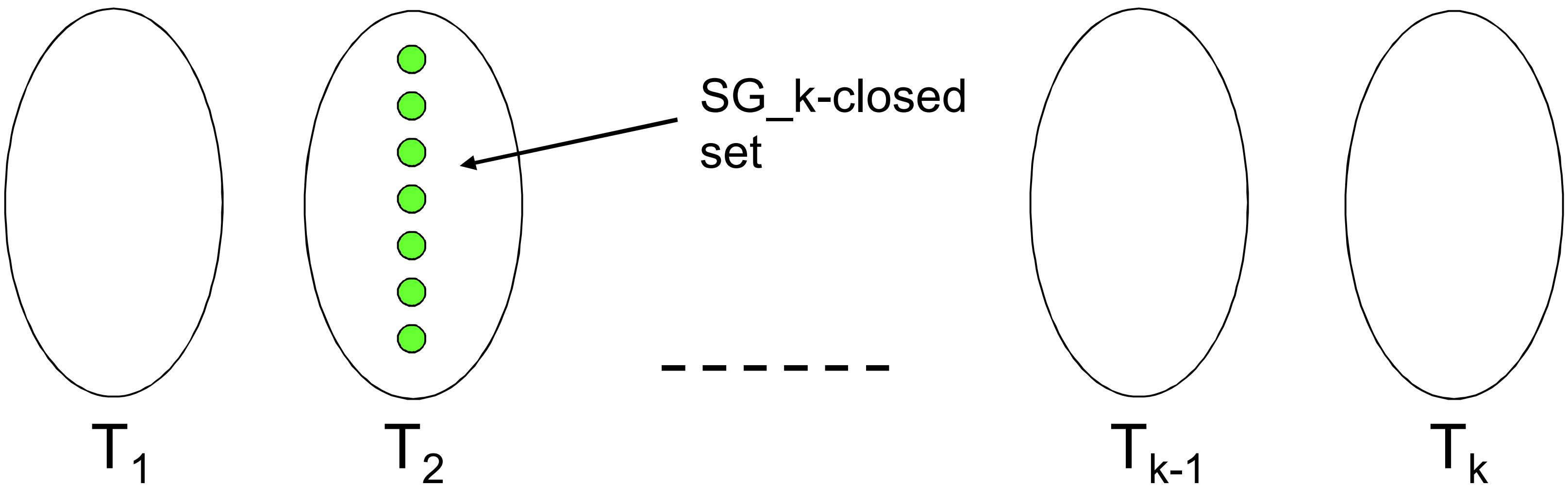
- We also prove SG_k(F,m) < k log m
  - Tight ONLY for F_2

SG → Rank

- Rank of depth-3 identity over F is…

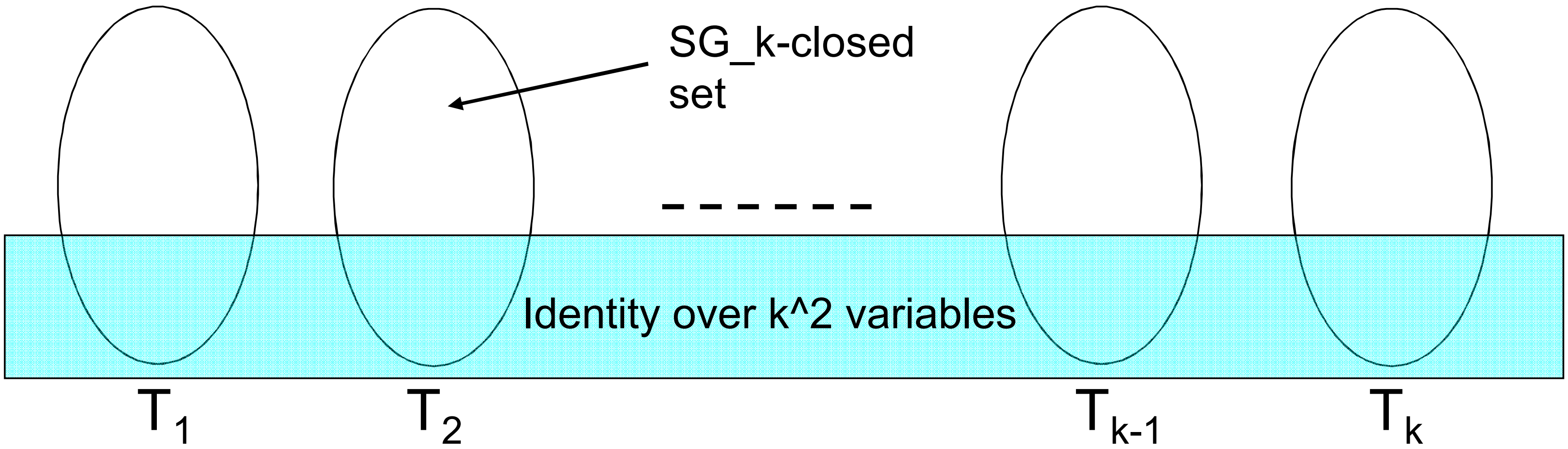
  k^2 + k SG_k(F,d)

$$C \equiv \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij} = \sum_{i=1}^{k} T_i$$



- So for F = Q,R Rank is O(k^2)
- For any F Rank is O(k^2 log d)

The nucleus identity



- [Structural theorem alert!]
- Every identity contains a nucleus identity of k^2 variables
- Everything else within a term is SG_k closed
    - All terms “look the same”
- All interesting complexity is inside nucleus

So…

- We prove that the rank of depth-3 identity is $k^2 + k\, SG_k(F,d)$
  - $O(k^2)$ for reals, setting DS conjecture
  - This is pretty much the end of the rank story

- Involves the kitchen sink of tools used for depth-3
  - [DS, KS, KS, KS, SS]

- Insight into depth-3 identities
  - The presence of the nucleus, the SG-relations

The road ahead

- Umm…solve identity testing
  - Surely, something intermediate…?

- Get truly polynomial (black-box or otherwise) for depth 3
  - How to remove exponential dependence on k?

- So we get d^k for R, but only d^{k log d} for general F
  - Can we get at least get polynomial in d in general?
  - Need different approach than rank bounds

- What about SG_k rank bounds?
  - (k log d) is just the beginning. Get better bound for finite fields.