Identities & Sylvester-Gallai Configurations

Nitin Saxena (Hausdorff Center for Mathematics, Bonn)

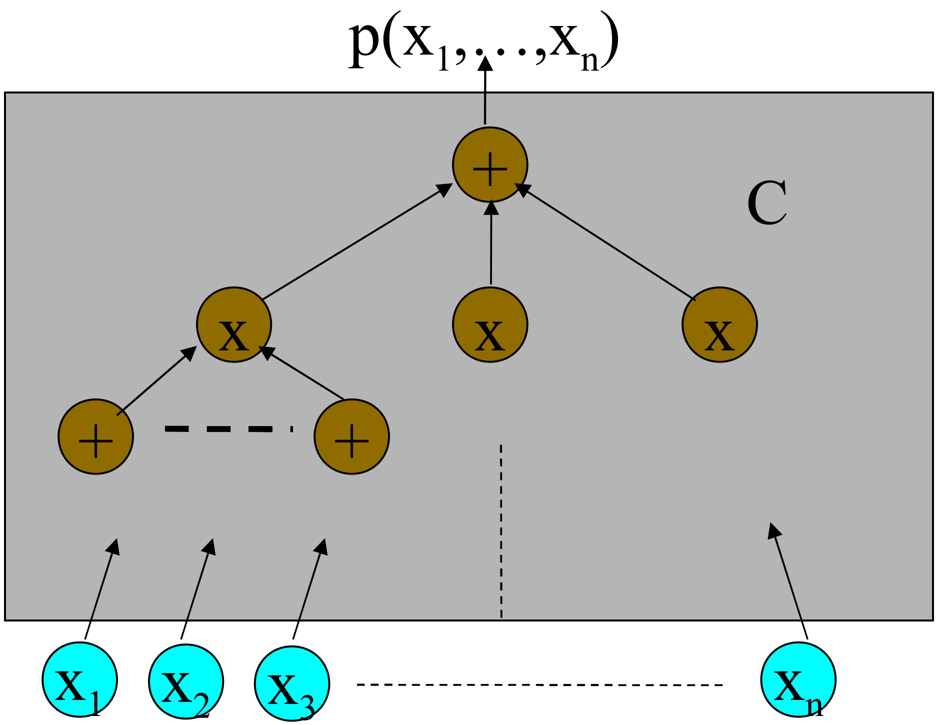
Joint work with

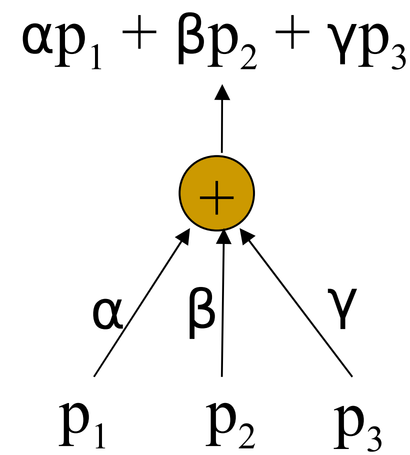
C. Seshadhri (IBM Almaden Research Center, San Jose)

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

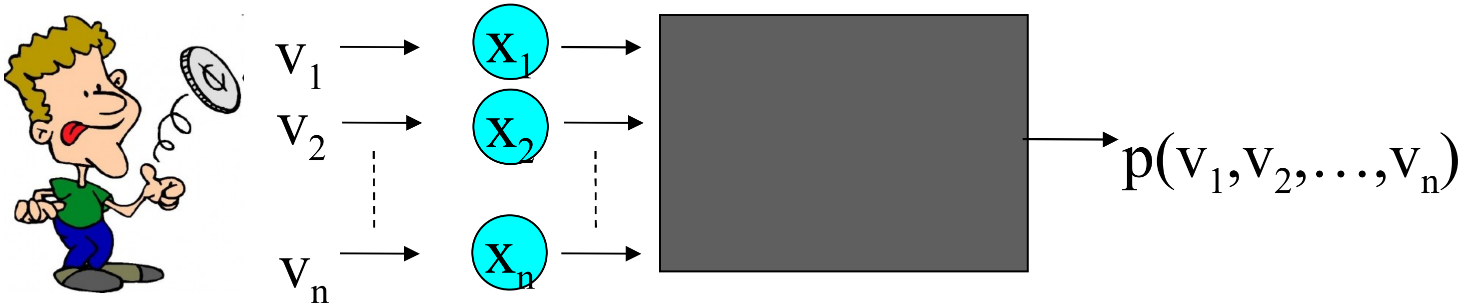




We want algorithm whose running time is polynomial in size of the circuit.

- Non blackbox: can analyze structure of C
- Blackbox: cannot look *inside* 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) open problem: Find a deterministic polynomial time algorithm.
  - We would really like a black box algorithm

Why?

- Come on, it's an interesting mathematical problem. Do you need a further reason?
- [Impagliazzo Kabanets 03] Derandomization implies circuit lower bounds for permanent

- [AKS] Primality Testing ; $(x + a)^n - x^n - a = 0 \pmod{n}$
- [L, MVV] Bipartite matching in NC?...
- Many more

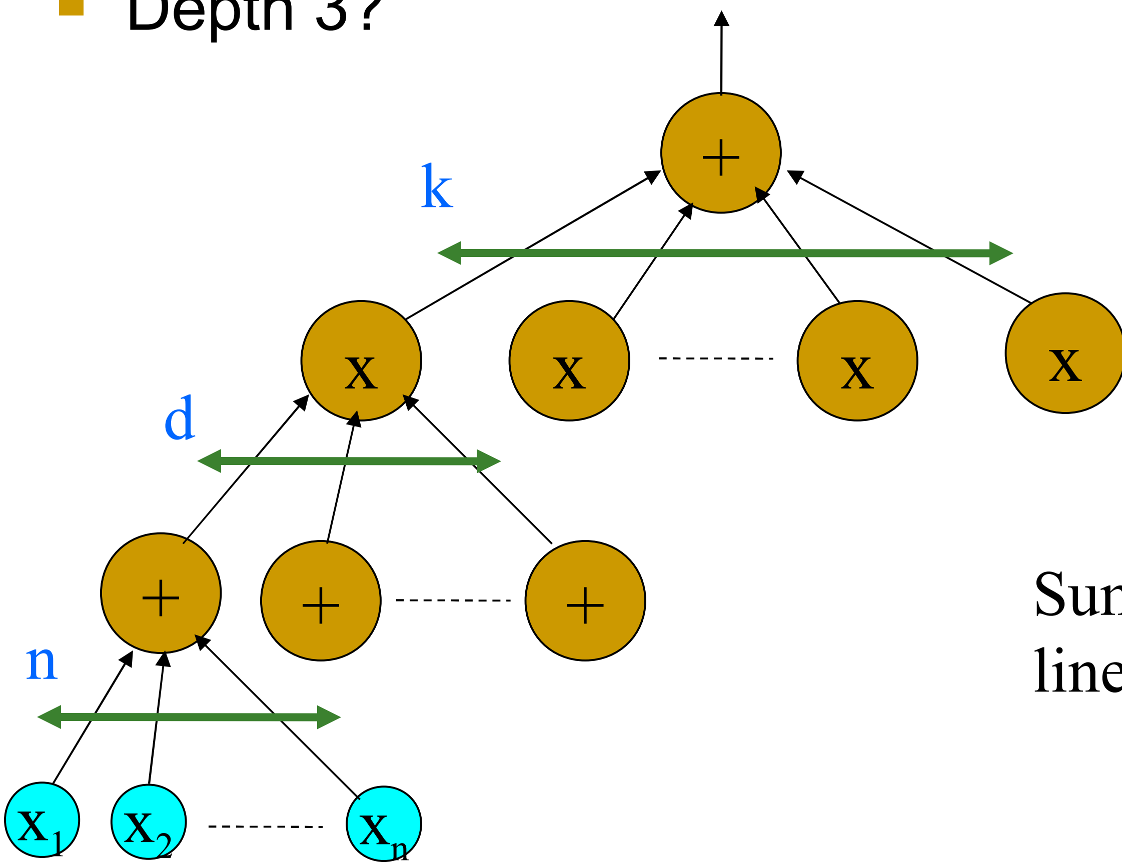
What do we do?

George Pólya 1887-1985

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!
  - [GK87, BOT88,…,KS01, A05] Polytime & blackbox
- Depth 3?

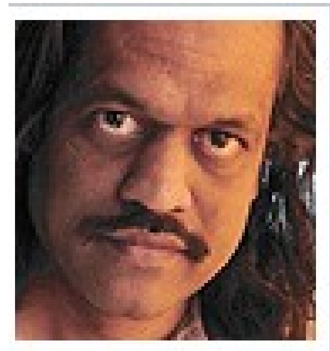


$$C = \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij} = \sum_{i=1}^{k} T_i$$

Sum of products of kd linear forms in n variables

Some good news

M. Agrawal



V. Vinay

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

- Build the bridge from depth 3 end!

The past…

- A ΣΠΣ(k,d,n) circuit: [redacted]

- [Dvir Shpilka 05] Non-blackbox poly(n)exp((log d)^k) algorithm.
- [Kayal Saxena 06] Non-blackbox poly(n,d^k) algorithm.

The past... [redacted]

A Tale of Three Methods

- [Karnin Shpilka 08] poly(n)exp((log d)^k) algorithm.
- [Saxena Seshadhri 09] poly(n)exp(k^3(log d)^2) algorithm.
- [Kayal Saraf 09] poly(n)exp(k^{k}log d) algorithm *over Q*.

- [Us] poly(n)exp(k^{2}log d) algorithm *over Q*.
  This almost matches the non-blackbox test!
- [Us] poly(n)exp(k^2(log d)^2) algorithm.

The rank

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

$$\begin{array}{cc} & n \\ M = \quad kd & \begin{bmatrix} \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \\ \\ \end{bmatrix} \end{array} \longleftarrow L_{ij} = \sum_{r=1}^{n} \alpha_r x_r$$

n-dim vector over F

Rank(C) = Rank (M)

- Introduced by [DS05]: fundamental property of depth 3 circuits
- [DS] Rank of *simple minimal* identity < (log d)$^{k-2}$ (compare with kd)
- How many independent variables can an identity have?
  - An identity is very constrained, so few degrees of freedom

What we did

- Rank of depth 3 (simple minimal) real identity < $3k^2$
  - There is identity with rank k, so this is almost optimal.
  - Over any field, we prove $3k^2(\log 2d)$.
- Therefore, [KS] gives det. blackbox $\exp(k^2 \log d)$ test.

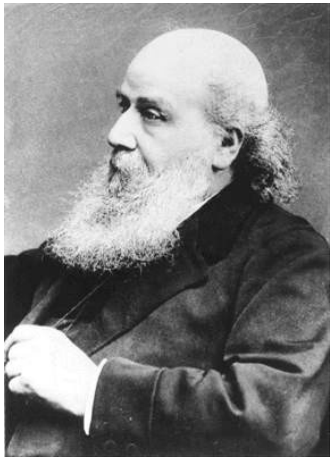
- We develop powerful techniques to study depth 3 circuits.
  - Probably more interesting/important than result.
- Every depth 3 identity contains a (k-1)-dim Sylvester-Gallai Configuration (SG_{k-1} config.).

To be simple and minimal

- Depth-3: $C = T_1 + T_2 + \ldots + T_k$
- Simplicity: no common (linear) factor for all T_r's
  - $x_1x_2\ldots x_n - x_1x_2\ldots x_n$ (Rank = n)
- Minimality: no subset of T_r's is identity
  - $x_1x_2\ldots x_nz_1 - x_1x_2\ldots x_nz_1 + y_1y_2\ldots y_nz_2 - y_1y_2\ldots y_nz_2$ (Rank = 2n+2)
- Strong minimality: $T_1, \ldots, T_{k-1}$ are linearly independent.

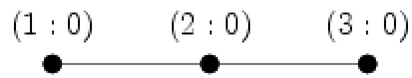
Meet Sylvester-Gallai (SG_2 Config.)

- Theorem: If $S \subset R^2$ is a finite set whose every two points lie on a line passing through a third point. Then S is collinear.
- This is a fundamental property of the field R.
  - It is not true for C^2.
- We abstract the following concepts out,
- SG_k-closed: $S \subset F^n$ such that for all linearly independent $v_1,\dots,v_k \in S$, there is another point of S in $\mathrm{span}(v_1,\dots,v_k)$.
- $SG_k(F,m)$: the largest rank of a SG_k-closed subset S ($|S| \le m$) of F^n.
- Rephrasing SG Theorem: $SG_2(R,m) \le 2$, for all m.

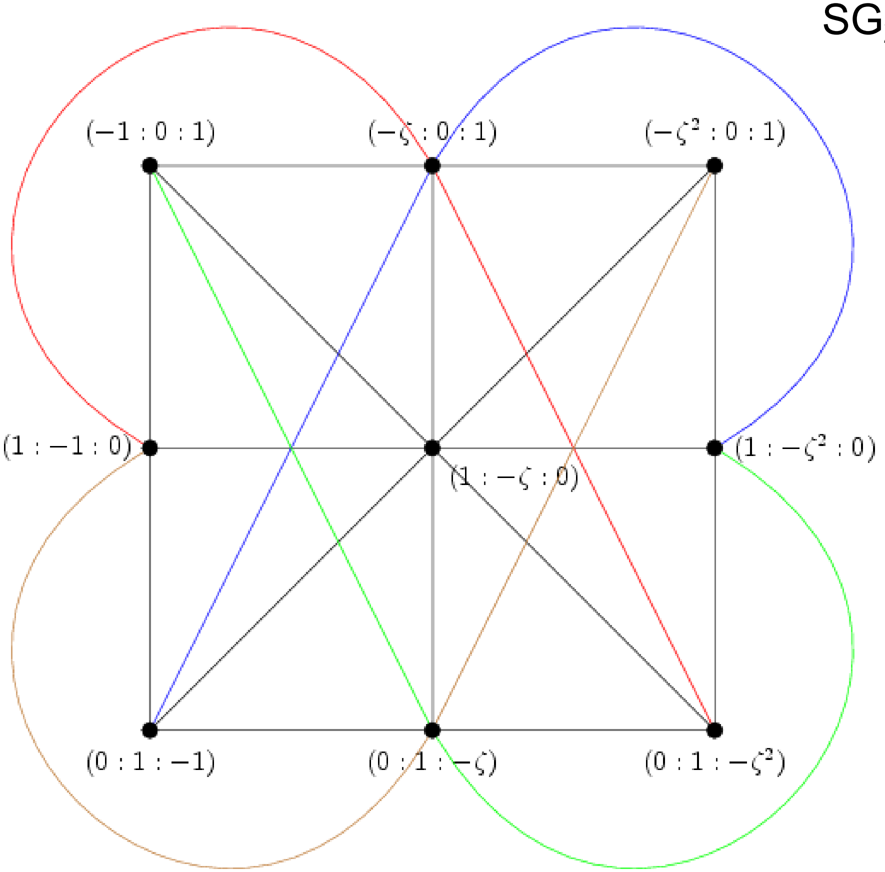


J. J. Sylvester 1814-1897

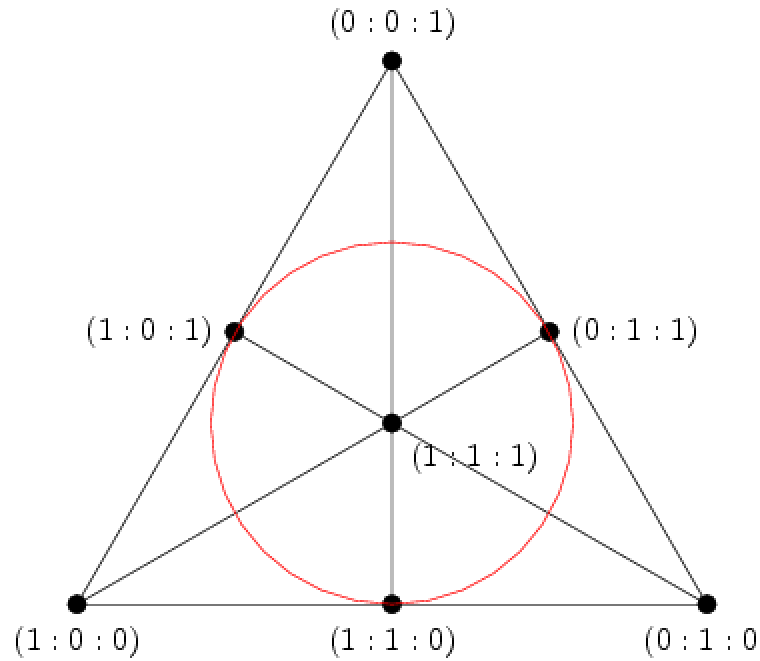
More Examples of SG_2 Config.



SG_2 Config. in R^n of rank 2



SG_2 Config. in C^n of rank 3



SG_2 Config. in F_2^n of rank 3

Higher dim Sylvester-Gallai

- Theorem [Hansen65, BE67]: $SG_k(R,m) \le 2(k-1)$.
- We feel that for any field F of zero char:

  $$SG_k(F,m) = O(k).$$

- $S := F_p^{\,r}$ is SG_2-closed. Thus $SG_2(F_p,m) = \Omega(\log_p m)$.
- We prove for any field: $SG_k(F,m) = O(k \log m)$.

Our Structure Theorem

- The rank of a simple, strongly minimal $\Sigma\Pi\Sigma(k,d)$ identity is : $SG_{k-1}(F,d) + 2k^2$.

- Let the identity be $C=T_1+...+T_k$. We show that forms in T_i yield a SG_{k-1}-configuration in F^n.
- Meta-Theorem: $\Sigma\Pi\Sigma(k)$ identity is an SG_{k-1}-configuration.

- From SG Theorems this gives rank bounds of:
  - $O(k^2)$ over reals.
  - $O(k^2 \log d)$ over all fields.

Where's the Beef ? k=3.

- $C = T_1 + T_2 + T_3 = \Pi L_i + \Pi M_j + \Pi N_k = 0$
- [AB99,AKS02,KS06] Go modulo!

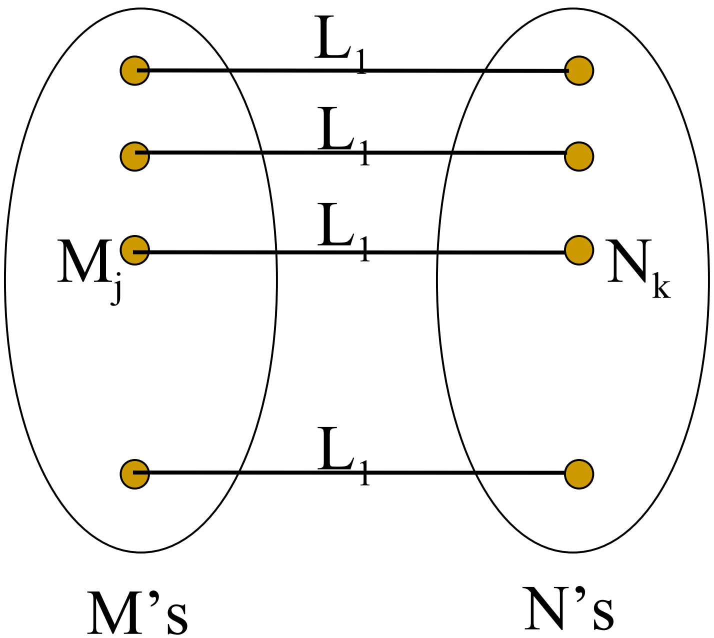
$$\prod L_i + \prod M_j + \prod N_k = 0$$

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

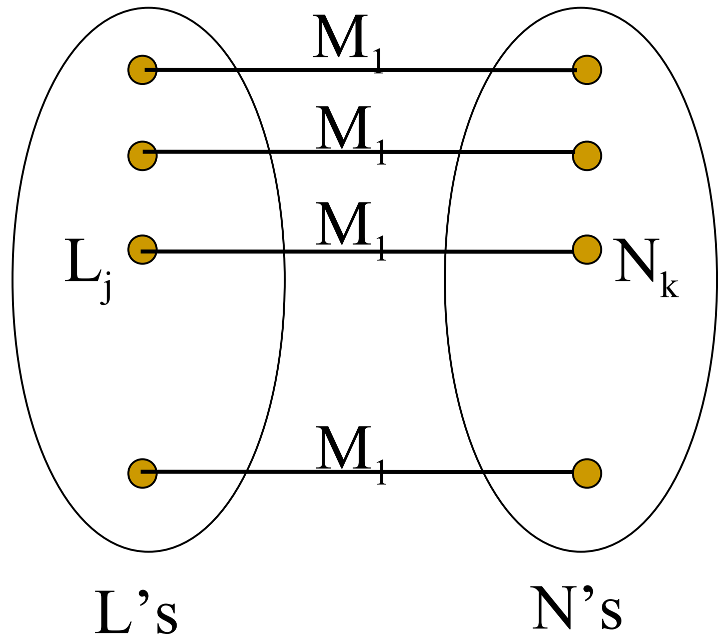
$$\prod M_j = -\prod N_k \pmod{L_1}$$

- By unique factorization, there is a bijection between M's and N's (they are same upto constants)
- This is the L_1 matching.

Matching all the Gates



and



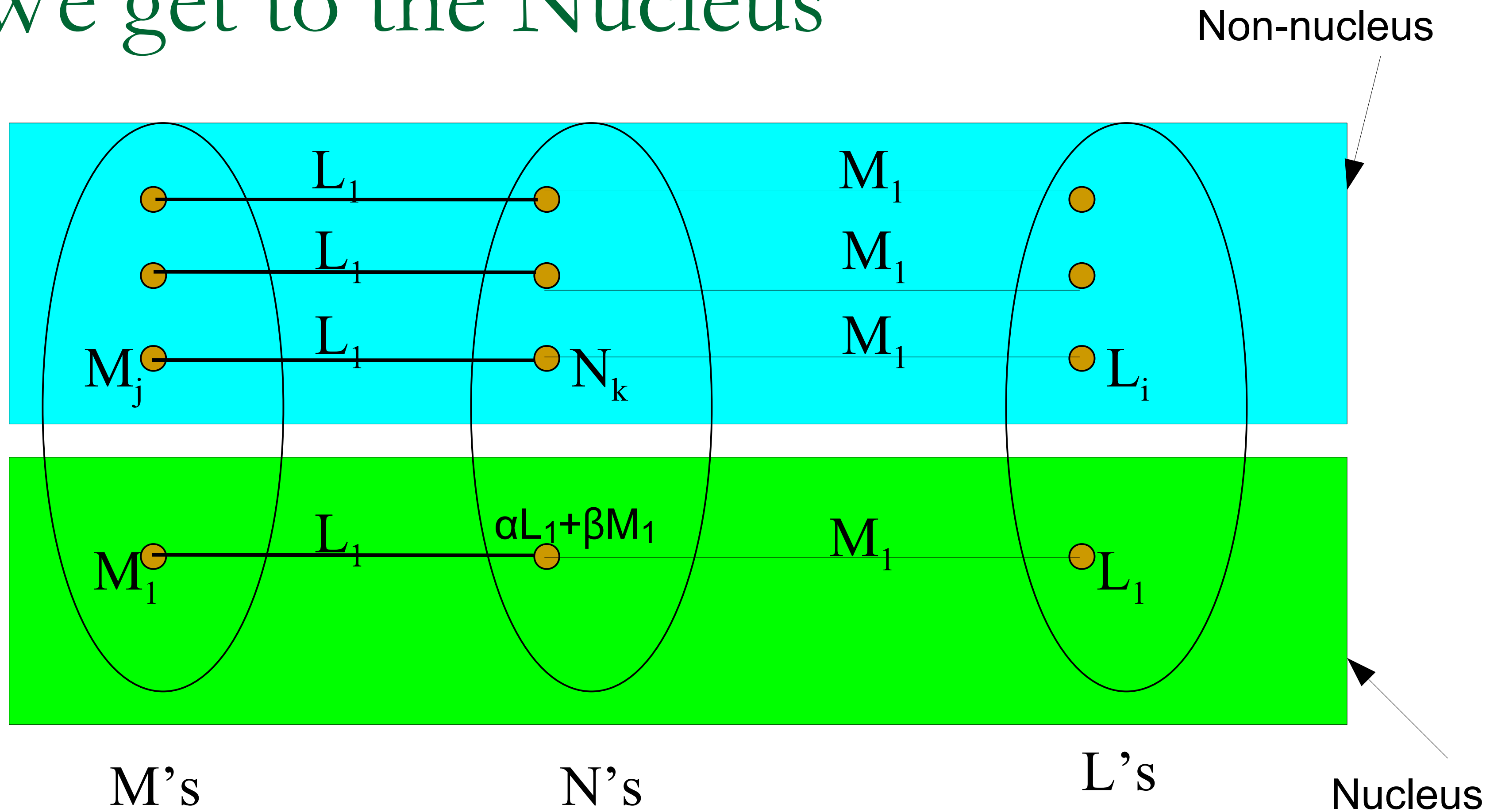
$M_j \equiv \alpha N_k \pmod{L_1}$

$M_j = \alpha N_k + \beta L_1$

$L_j \equiv \alpha' N_k \pmod{M_1}$

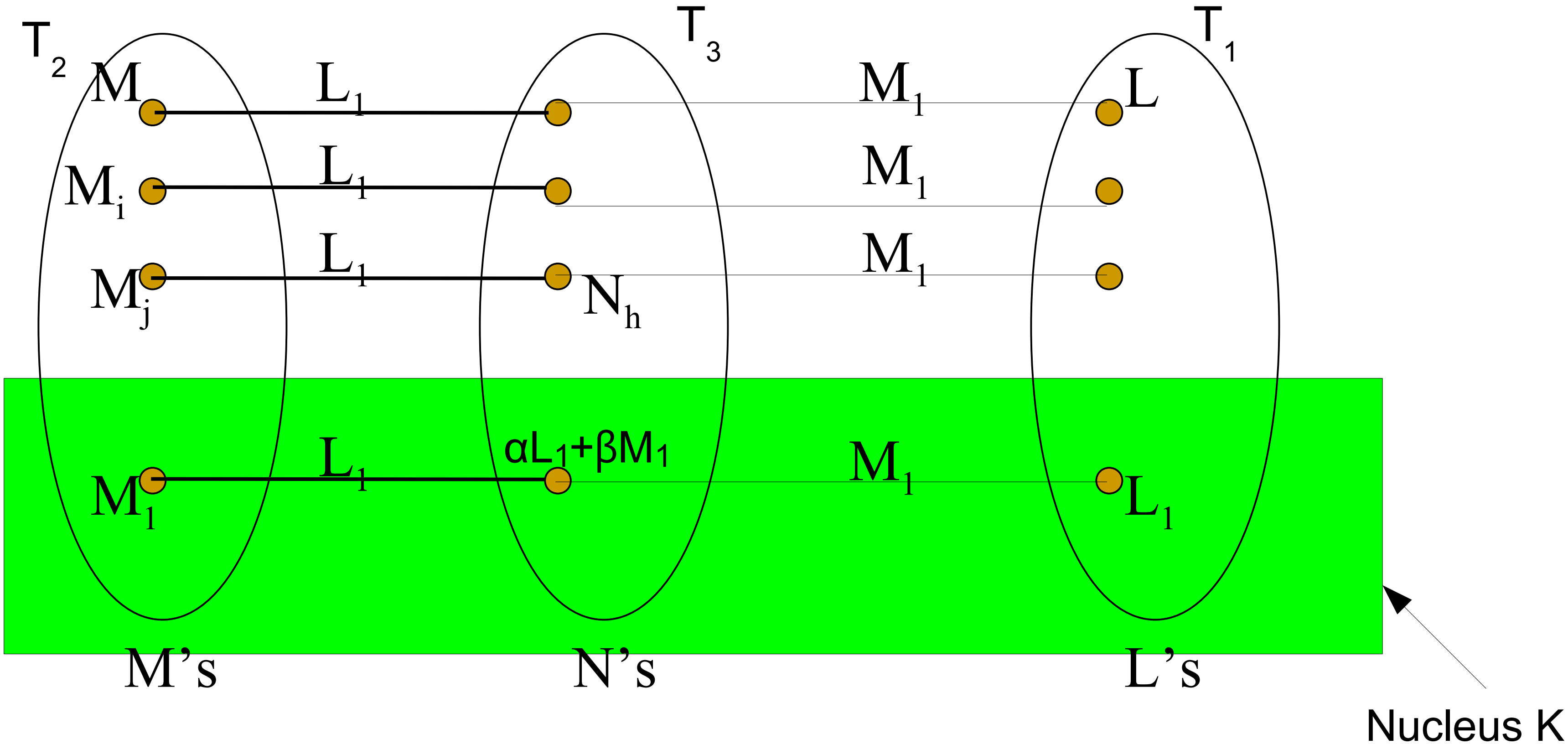
$L_j = \alpha' N_k + \beta' M_1$

We get to the Nucleus



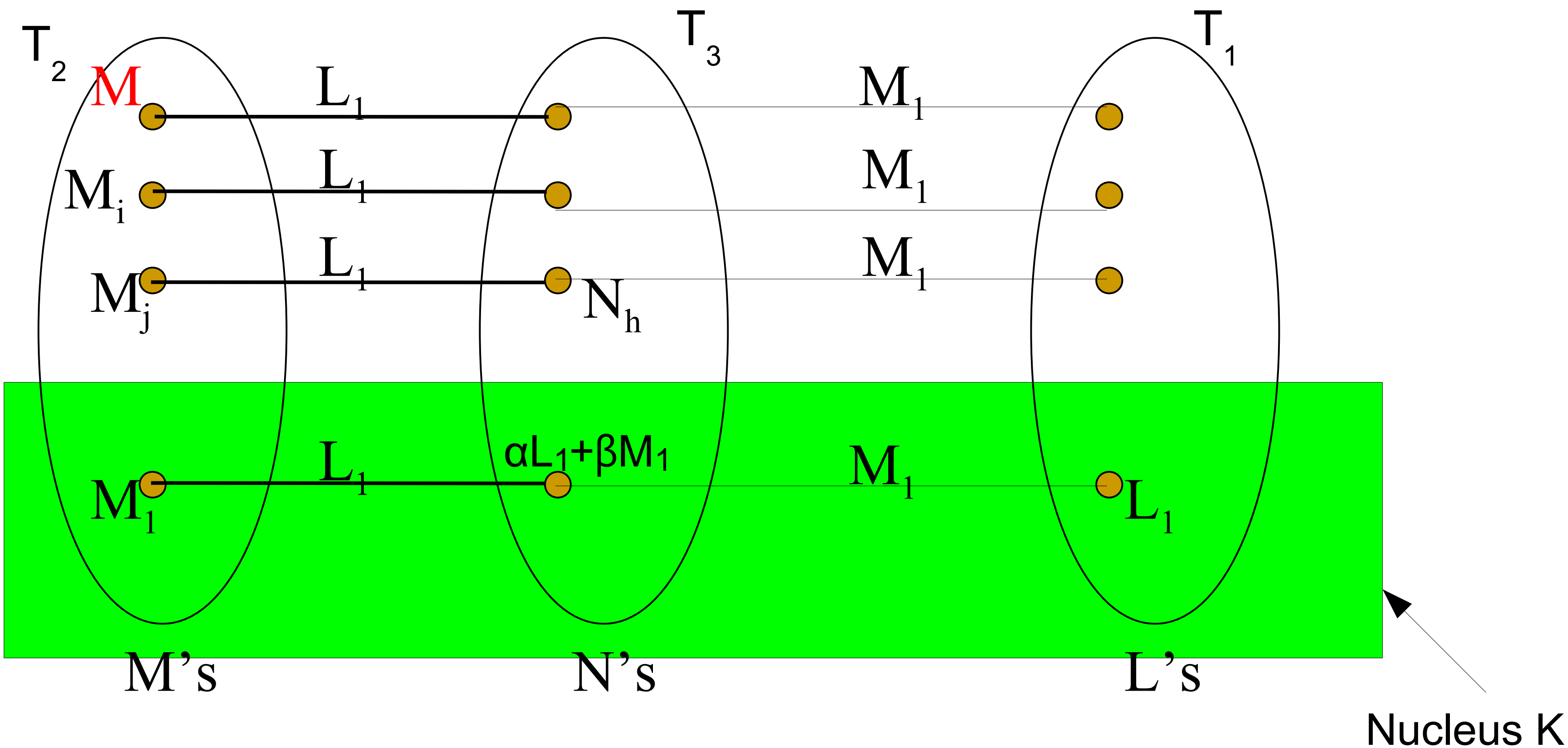
- Forms in nucleus are in span(L_1,M_1)=:K.
- Forms in non-nucleus are matched mod K.

Proof Idea



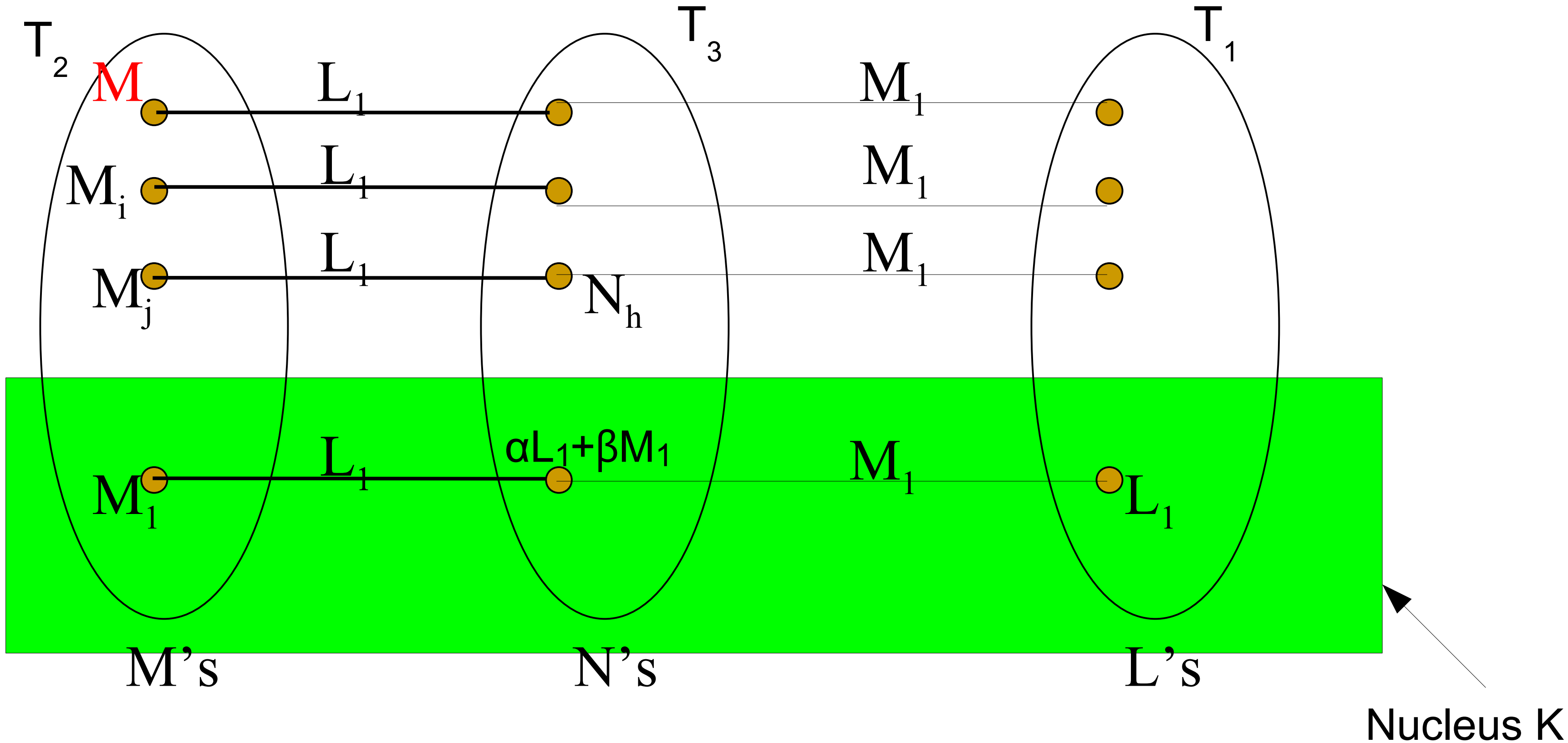
- Pick M_i, M_j non-similar mod K.
- $T_1 \equiv 0 \pmod{M_i, N_h}$
- There exists L in T_1 s.t. $L = \alpha M_i + \beta N_h$
- Its image M satisfies : M (mod K) $\in$ span(M_i, M_j)

Proof Idea (Contd.)



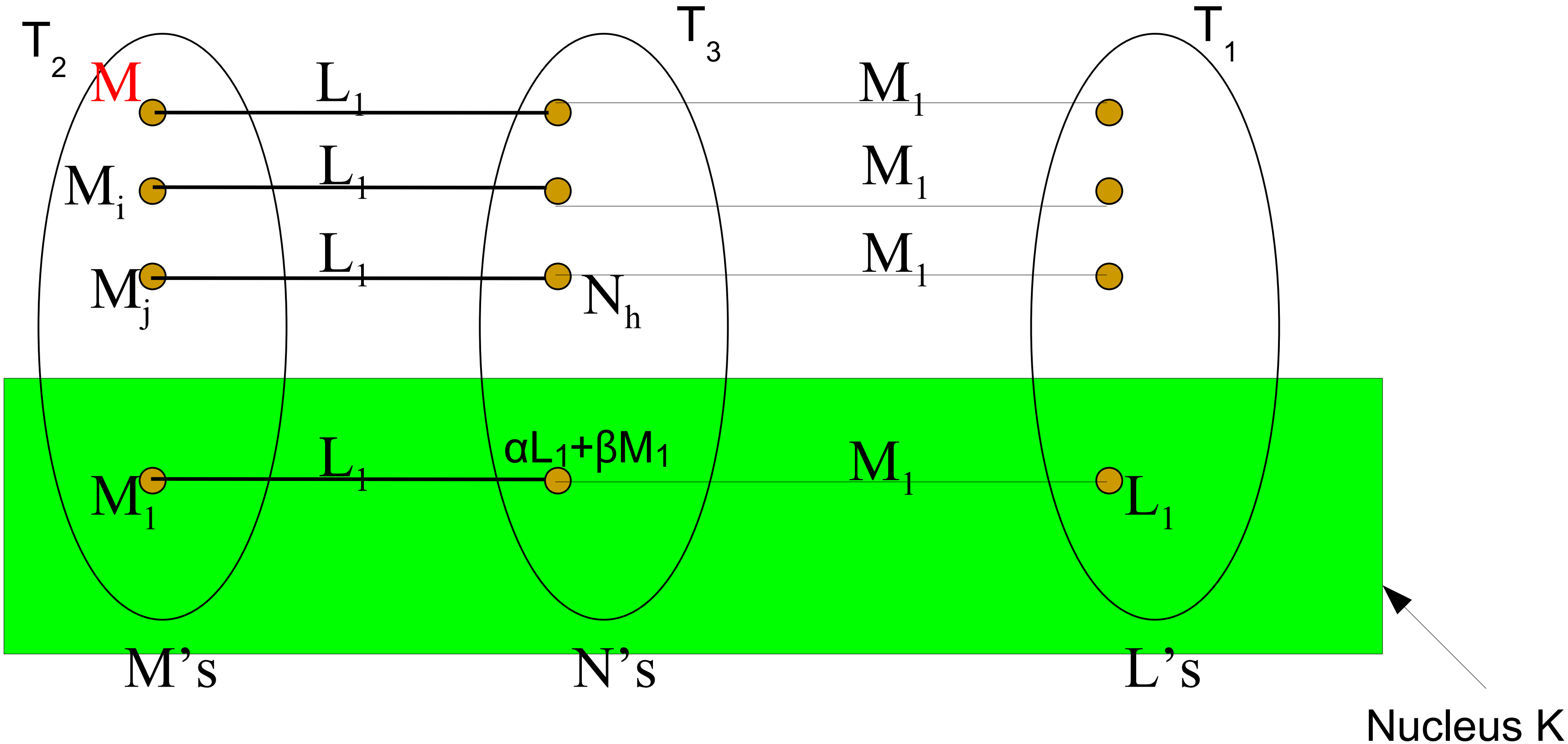
- M (mod K) $\in$ span(M_i, M_j)
- The non-nucleus part of T_i is SG_2-closed (mod K).
- Explicitly, the map $(\sum \alpha_i x_i) \mapsto (\alpha_1,\dots,\alpha_n)$ converts linear forms to a SG_2-closed subset of F^n/K.

Proof Idea (Contd.)



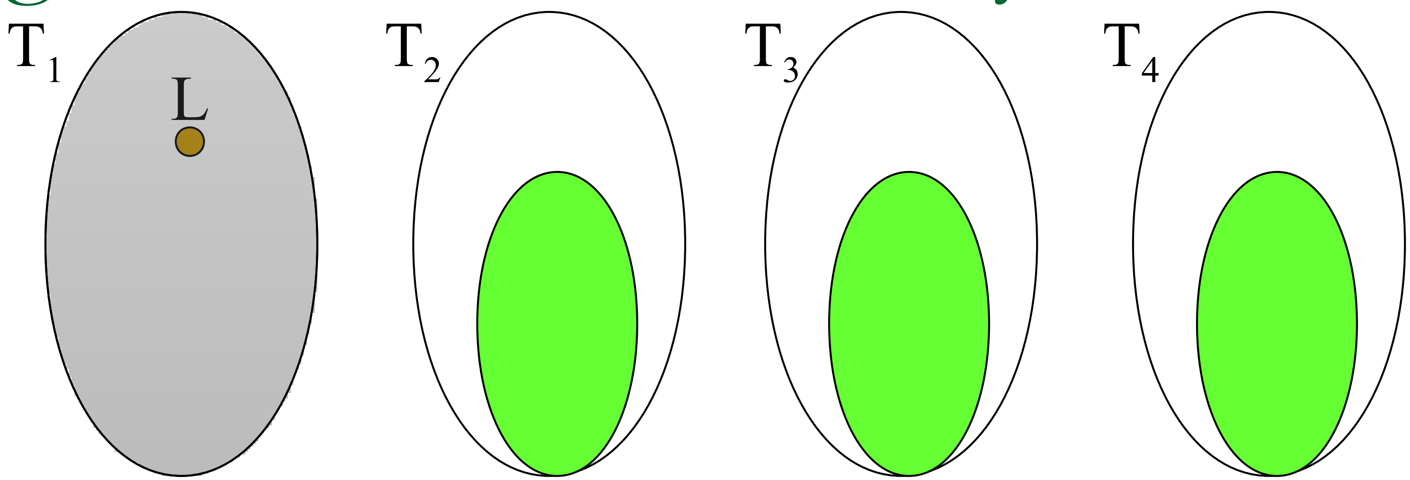
- The non-nucleus part of T_i is SG_2-closed (mod K).
- Rank of this identity $\leq 2 + SG_2(F,d)$
  - Over reals, $\leq 2 + 2 = 4$
  - Any field, $\leq 2 + \log d = O(\log d)$

A Bonus...



- The non-nucleus part of T_i is SG_2-closed (mod K).
- By degree comparison, the green part forms a subidentity.
- The nucleus part is a simple minimal subidentity.

Larger k: can't induct easily

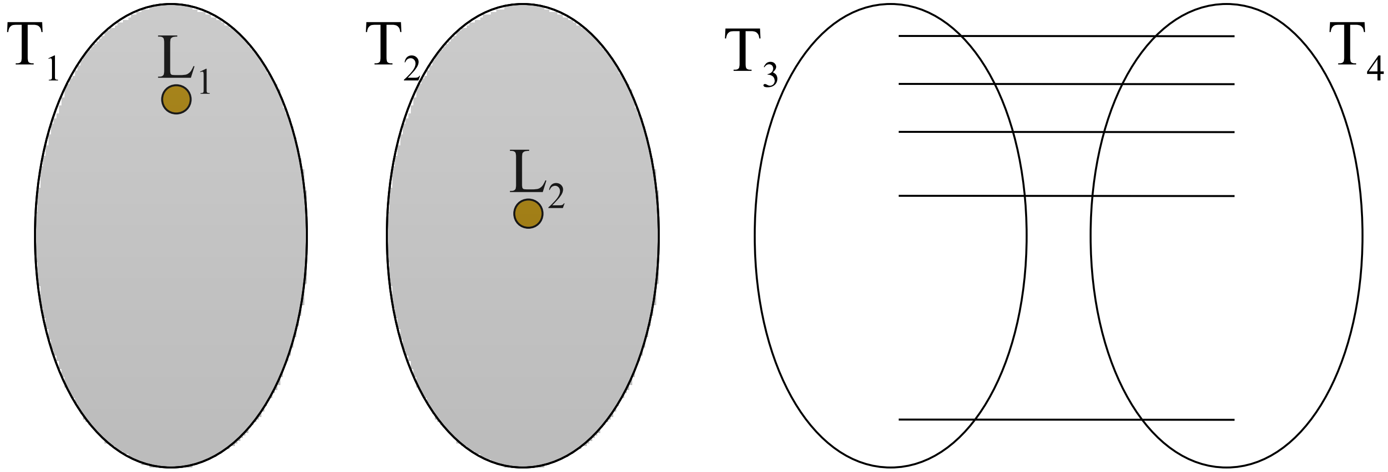


- $C = T_1 + T_2 + T_3 + T_4$
- $L \in T_1$. So how about $C \pmod{L}$? Top fanin is now 3.
- But $C \pmod{L}$ may not be simple or minimal any more!
  - $x_1x_2 + (x_3-x_1)x_2 + (x_4-x_2)x_3 - x_3x_4$
  - Going $\pmod{x_1}$, we get $x_2x_3 + (x_4-x_2)x_3 - x_3x_4$

The ideal way to Matchings

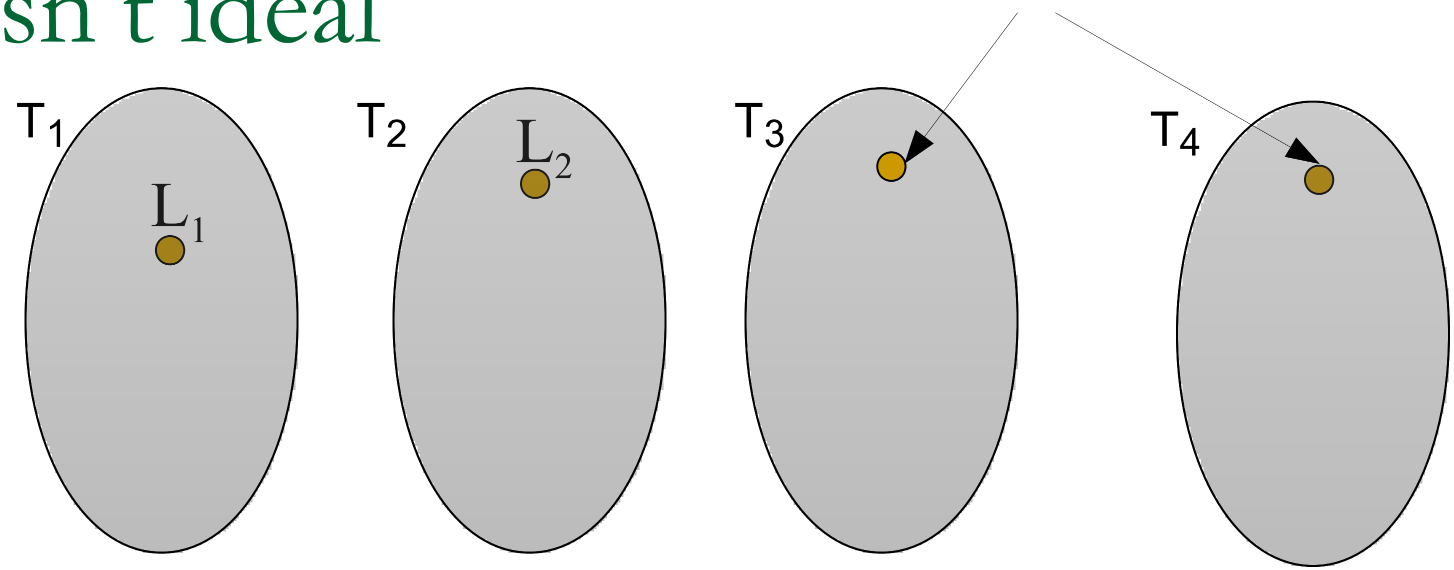
- We'll avoid induction and attack directly!
- We saw the power of matchings for k=3
- We extend matchings to ideal matchings for all k
  - Looking at C modulo an ideal, not just a linear form

Ideal matchings



- C (mod L_1, L_2) or C (mod I)
  - I is ideal <L_1, L_2>
- $T_3 + T_4 = 0$ (mod I)
  - By unique factorization, we get I-matching

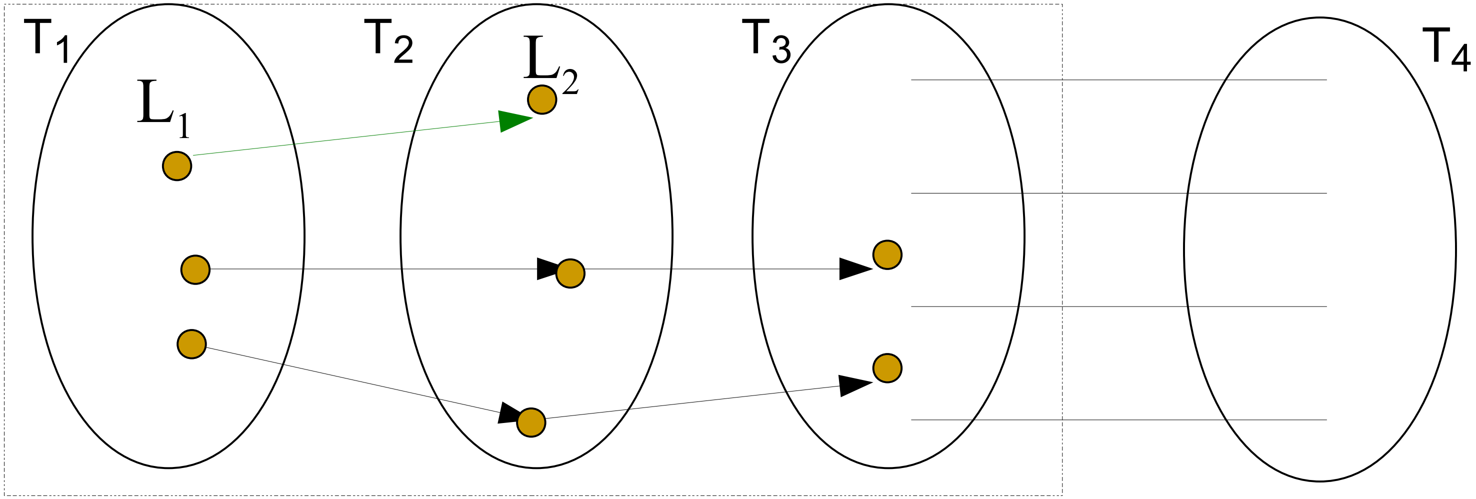
Life isn't ideal



- C (mod L_1, L_2) has no terms (i.e. we get 0=0)
- How can we get a matching?

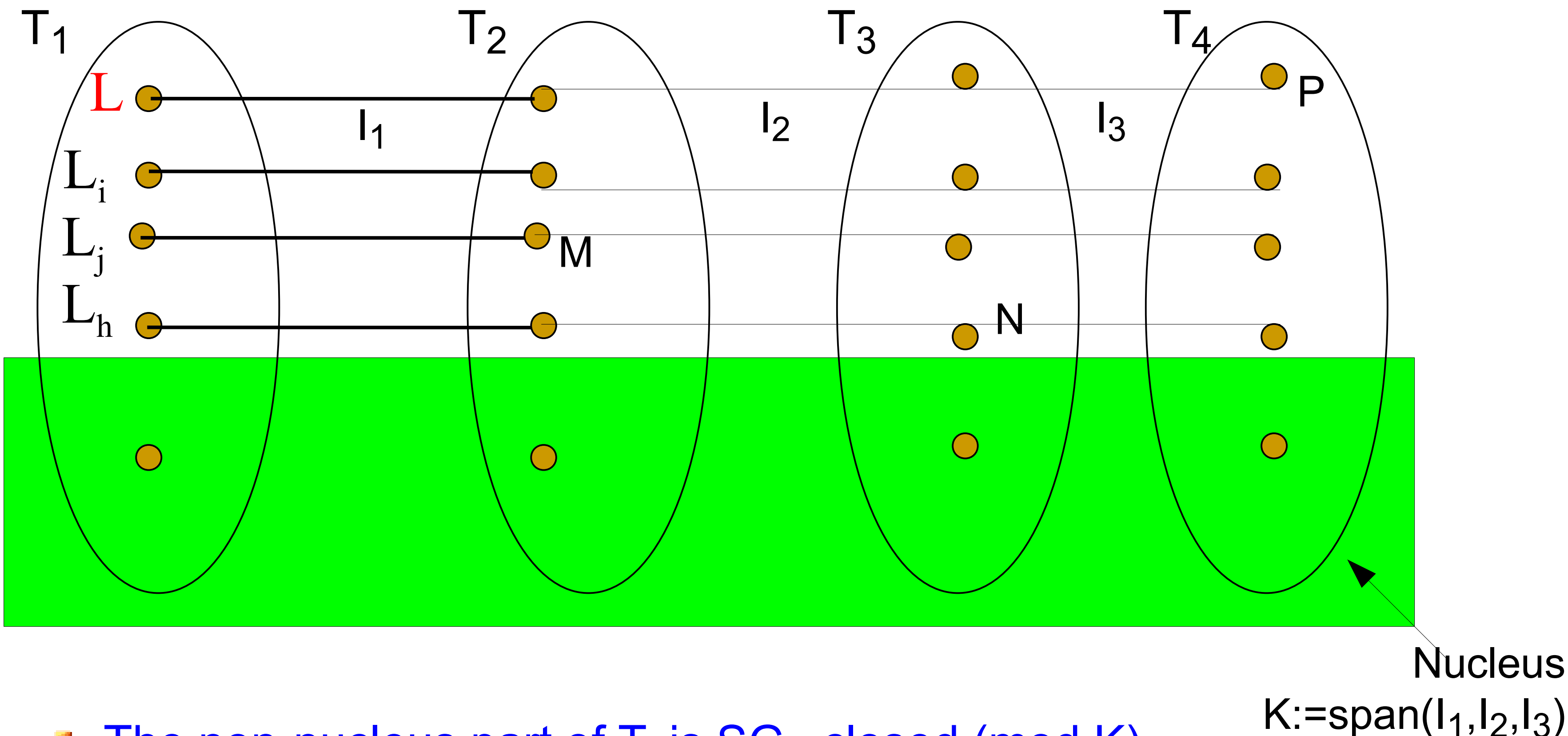
- We need L_1, L_2 s.t. T_3 (mod L_1, L_2) is nonzero.

The Right Path



- We need L_1, L_2 s.t. T_3 (mod L_1, L_2) is nonzero.
- By minimality of C, $T_1+T_2+T_3 \neq 0$.
- A generalization of [KS06]'s non-blackbox ideas ensures the existence of a path $\{L_1, L_2\}$ not hitting T_3.
- Now $T_3+T_4=0$ (mod L_1,L_2) is nontrivial and matches.

Summing Up...



- The non-nucleus part of T_i is SG_3-closed (mod K).
- Rank of this identity ≤ (rk K)+ SG_3(F,d)
- This idea (with a lot of work!) gives ≤ $2k^2$+ SG_{k-1}(F,d)
- The nucleus part is a simple, strongly minimal subidentity.

In conclusion…

- Interesting matching & geometric structures in depth 3 identities.
  - Combinatorial view of algebraic properties
- Every depth 3 identity hides a nucleus subidentity.
  - Can we characterize the nucleus?
- $SG_k(F,d)$ is a fundamental property of fields.
  - Is $SG_k(F,d)=O(k)$ for fields of zero char. (large char.) ?

A Saxena-Seshadhri paper