

Reconstruction of Depth 3 Arithmetic circuits with Top Fanin 3

CCC August, 2025

Shubhangi Saraf, Devansh Shringi
University of Toronto

Arithmetic Circuits

- Circuit computing a polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$.
- Gates are $+$, \times .
- Leaves have $\{x_1, \dots, x_n, \mathbb{F}\}$.
- Edges with labels from \mathbb{F} (1 by default).

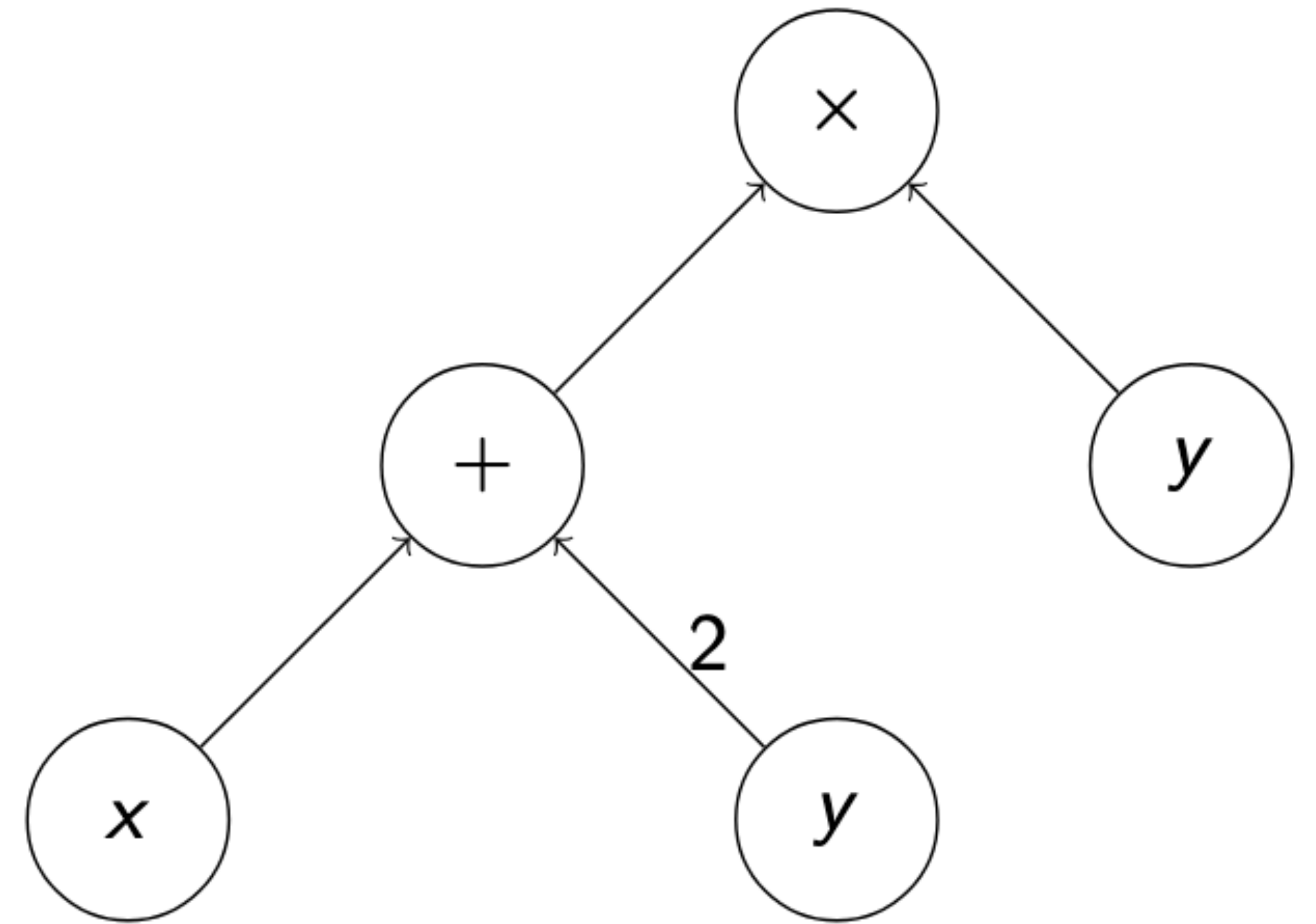


Figure: Circuit computing $xy + 2y^2$

Reconstruction

- $f \in \mathbb{F}[x_1, \dots, x_n]$ computed by $C \in \mathcal{C}$.
- Given Blackbox access to evaluations of f .
- Efficiently output a circuit C' that computes f .

Reconstruction

- $f \in \mathbb{F}[x_1, \dots, x_n]$ computed by $C \in \mathcal{C}$.
- Given Blackbox access to evaluations of f .
- Efficiently output a circuit C' that computes f .

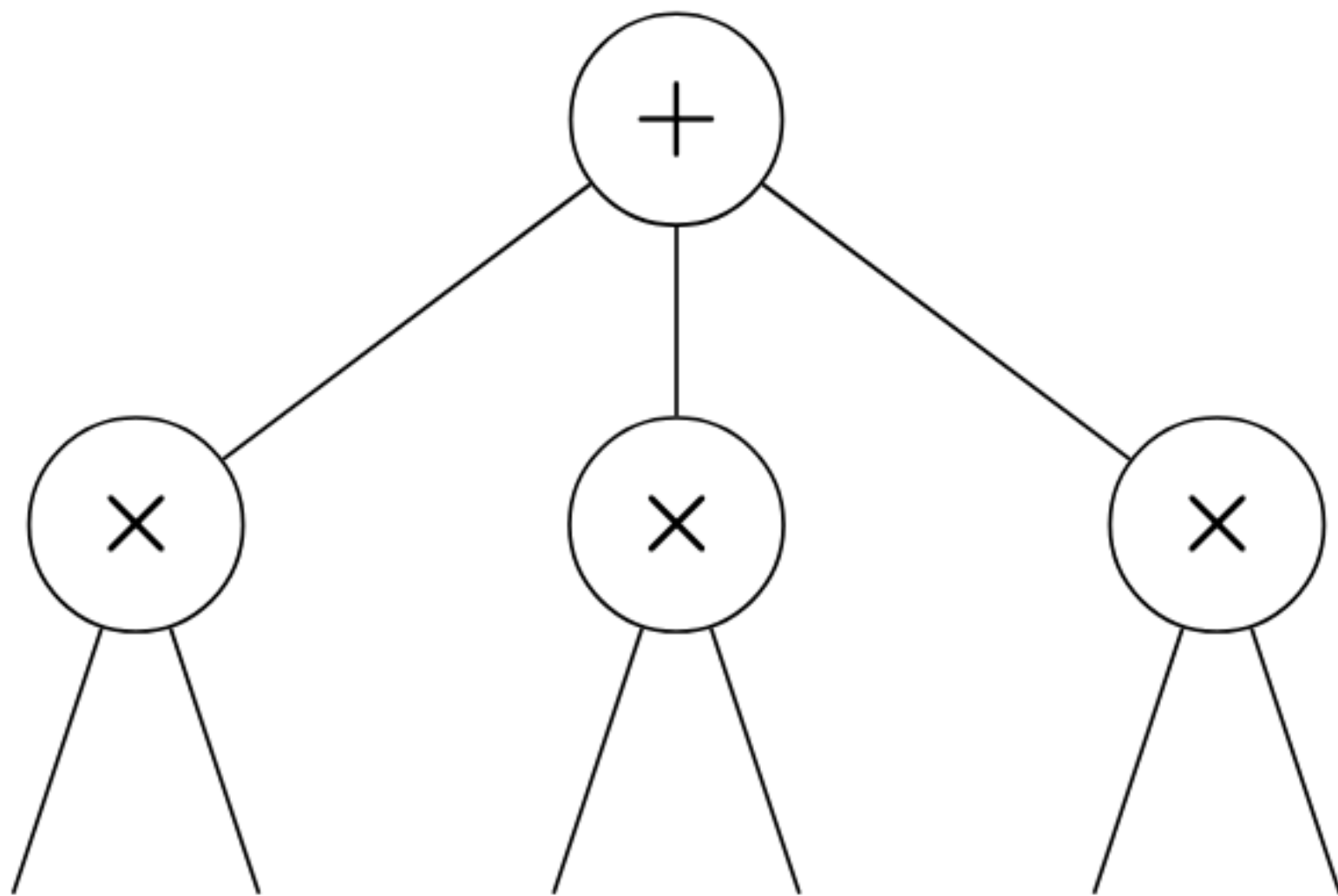
[Proper Learning]: If $C' \in \mathcal{C}$

Depth 2 Circuits

Depth 2 Circuits

$\Sigma\Pi$ Circuit

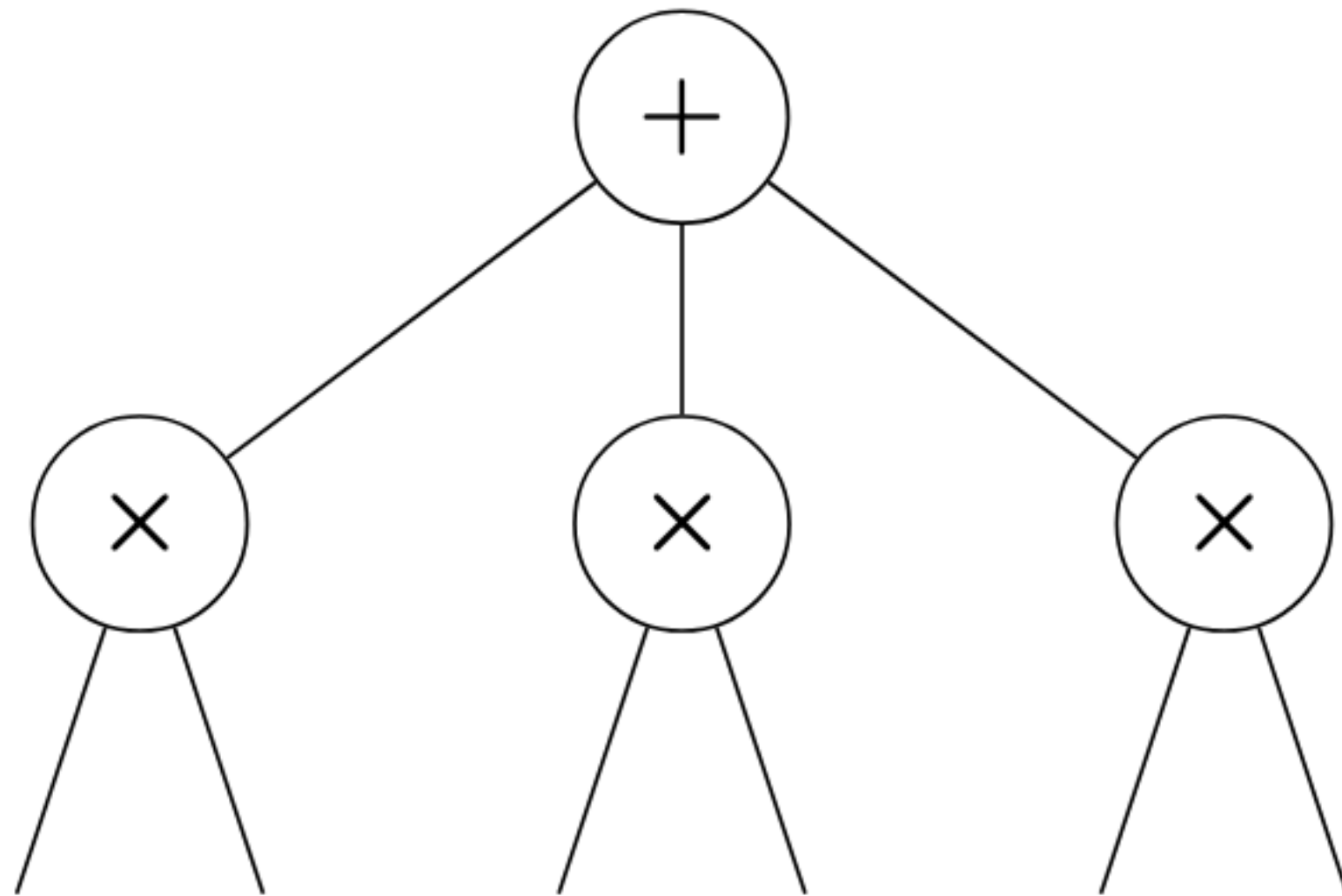
- Multivariate Interpolation [BOT83, KS01]



Depth 2 Circuits

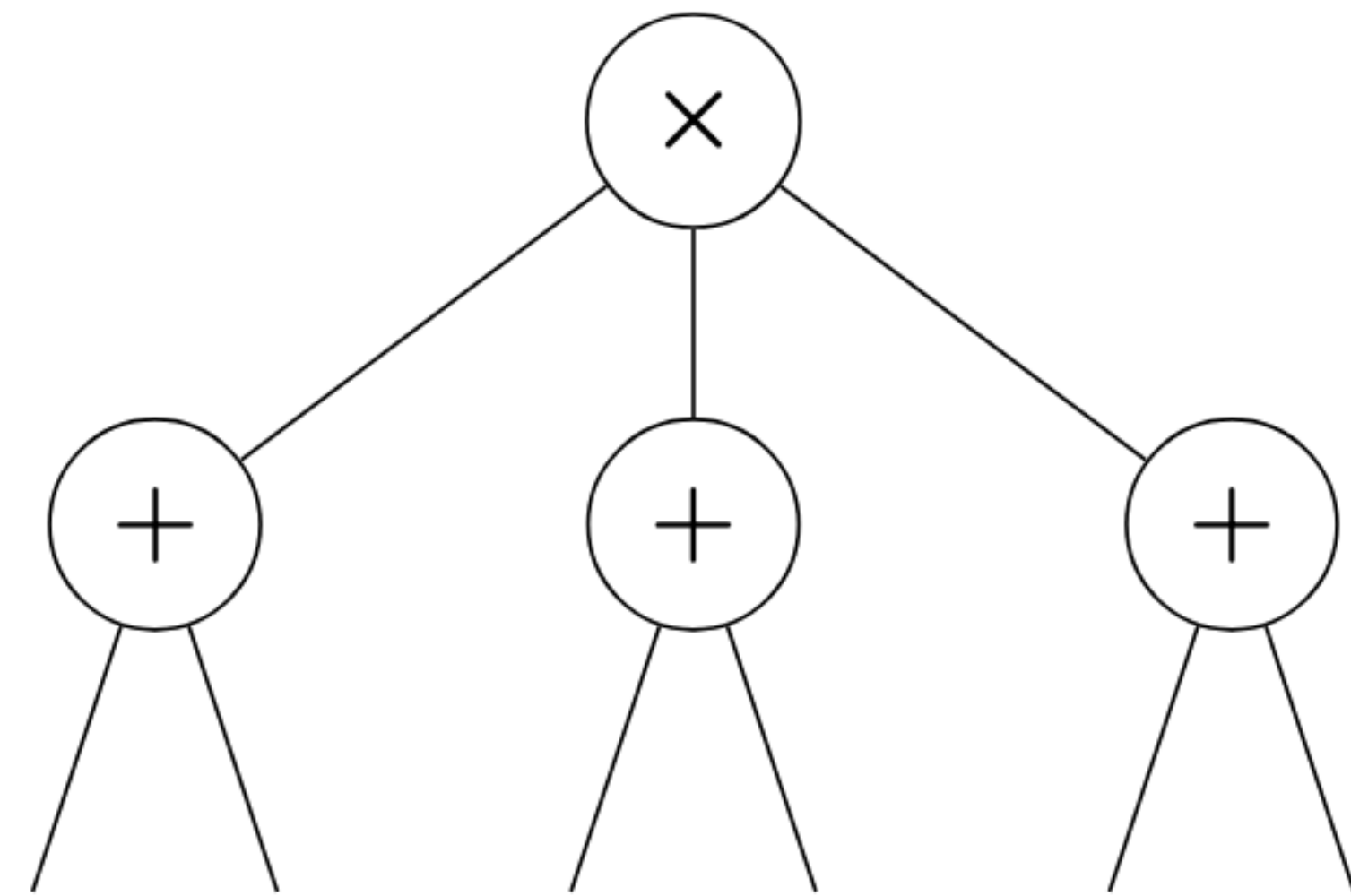
$\Sigma\Pi$ Circuit

- Multivariate Interpolation [BOT83, KS01]



$\Pi\Sigma$ Circuit

- Factoring [Kal87]



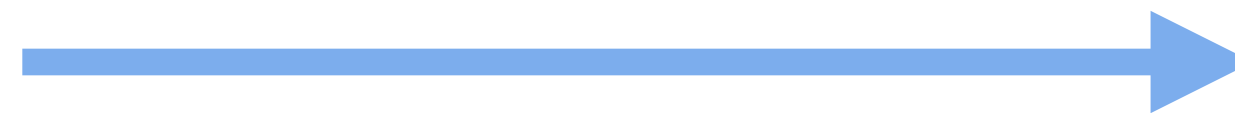
Depth 3 Circuits

- Combination of Factoring and Interpolation work for $\Pi\Sigma\Pi$ circuits
- Extremely challenging for $\Sigma\Pi\Sigma$ circuits.
- Reconstruction for Set-Multilinear $\Sigma\Pi\Sigma$ circuits captures [Tensor Decomposition](#).
- [\[Open\]](#): Proper Learning for $\Sigma\Pi\Sigma$ circuits with Top Fan-in 2 and $n = 5$

Hardness for Reconstruction of $\Sigma\Pi\Sigma$ Circuits

- Depth Reduction [GKKS13]

Polytime Reconstruction
For $\Sigma\Pi\Sigma$ circuits

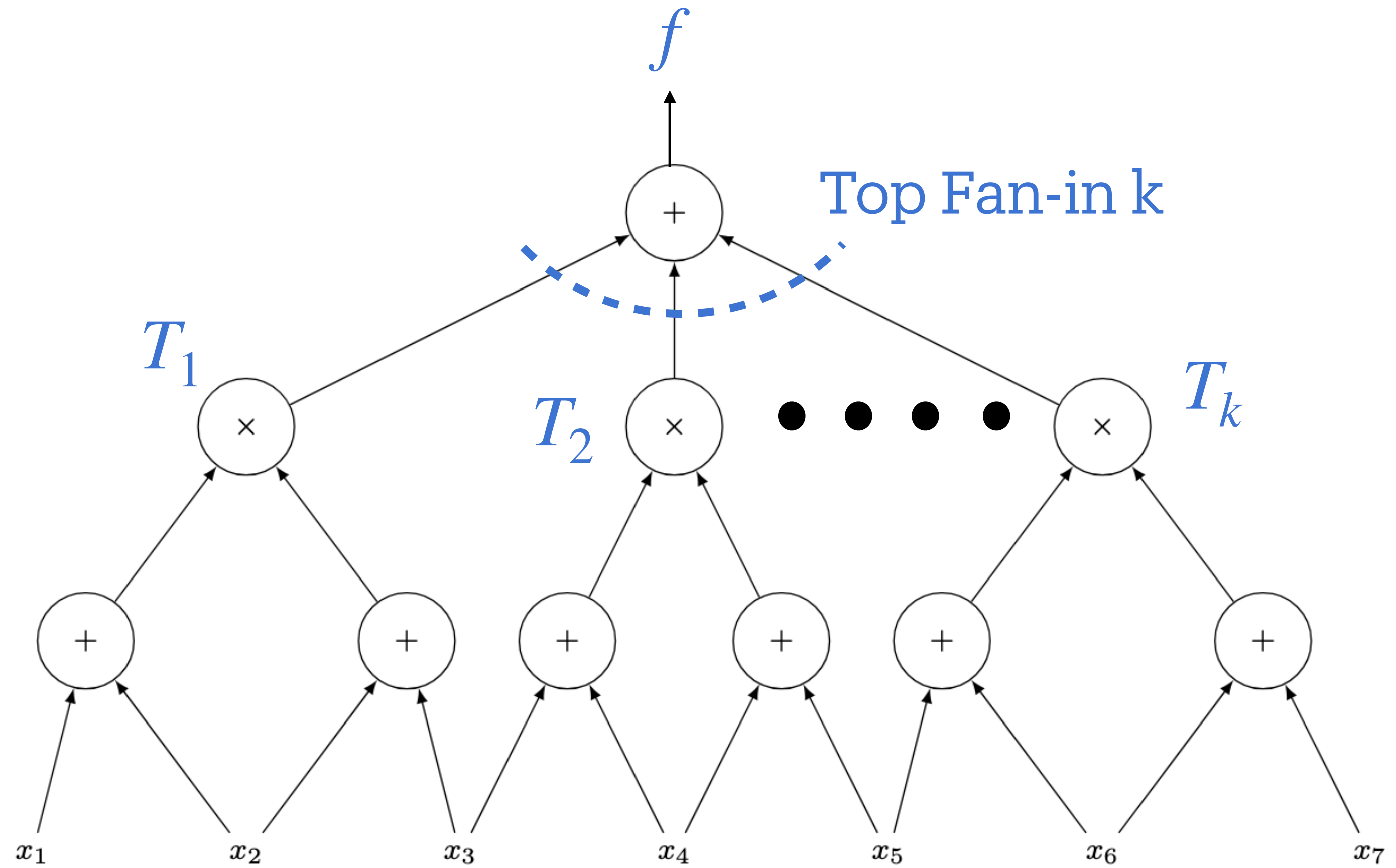


Subexponential Reconstruction
For General circuits

- Polytime PAC Learning for $\Sigma\Pi\Sigma$ circuits breaks cryptographic primitives [KS06].
- Proper Learning for Set-Multilinear $\Sigma\Pi\Sigma$ circuits is NP-hard[Häs90].

Depth 3 Circuits

With Restricted Fan-in



Depth 3 Circuits

- Restricted Top Fan-in $\Sigma\Pi\Sigma(k)$ circuits

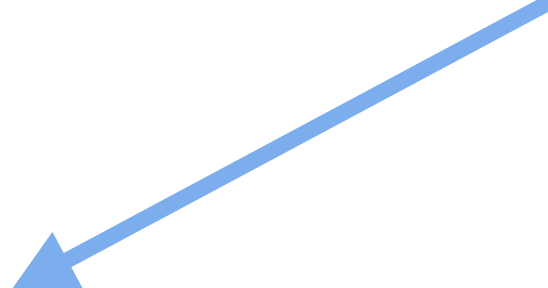
Depth 3 Circuits

- Restricted Top Fan-in $\Sigma\Pi\Sigma(k)$ circuits

$$C = G \times (T_1 + T_2 + \dots + T_k)$$

where each $T_i = \prod_{j=1}^d l_{ij}$ and $\gcd(T_1, \dots, T_k) = 1$

sim(C)



Depth 3 Circuits

- Restricted Top Fan-in $\Sigma\Pi\Sigma(k)$ circuits

sim(C)

$$C = G \times (T_1 + T_2 + \dots + T_k)$$

where each $T_i = \prod_{j=1}^d l_{ij}$ and $\gcd(T_1, \dots, T_k) = 1$

- $\text{rank}(\text{sim}(C)) = \dim(\text{span}(\{l_{ij} : i \in [k], j \in [d]\}))$

Polynomial Identity Testing (PIT)

- Checking if the input circuit computes 0 or not
- Simple Randomized Solution [Sch80, Zip79]
- **Open**: Efficient Derandomization

Polynomial Identity Testing (PIT)

- Checking if the input circuit computes 0 or not
- Simple Randomized Solution [Sch80, Zip79]
- **Open**: Efficient Derandomization
- Easier than Deterministic Reconstruction.

PIT for $\Sigma\Pi\Sigma(k)$ Circuits

- Connections to Discrete Geometry, specifically SG-configurations.

The diagram shows the equation $C = T_1 + T_2 + T_3 = 0$. Each tensor is represented by a vertical rounded rectangle containing colored dots. T_1 contains 10 red dots, T_2 contains 10 blue dots, and T_3 contains 10 green dots. The dots are arranged in a way that suggests they are vectors in a 2D plane, and their sum is zero.

PIT for $\Sigma\Pi\Sigma(k)$ Circuits

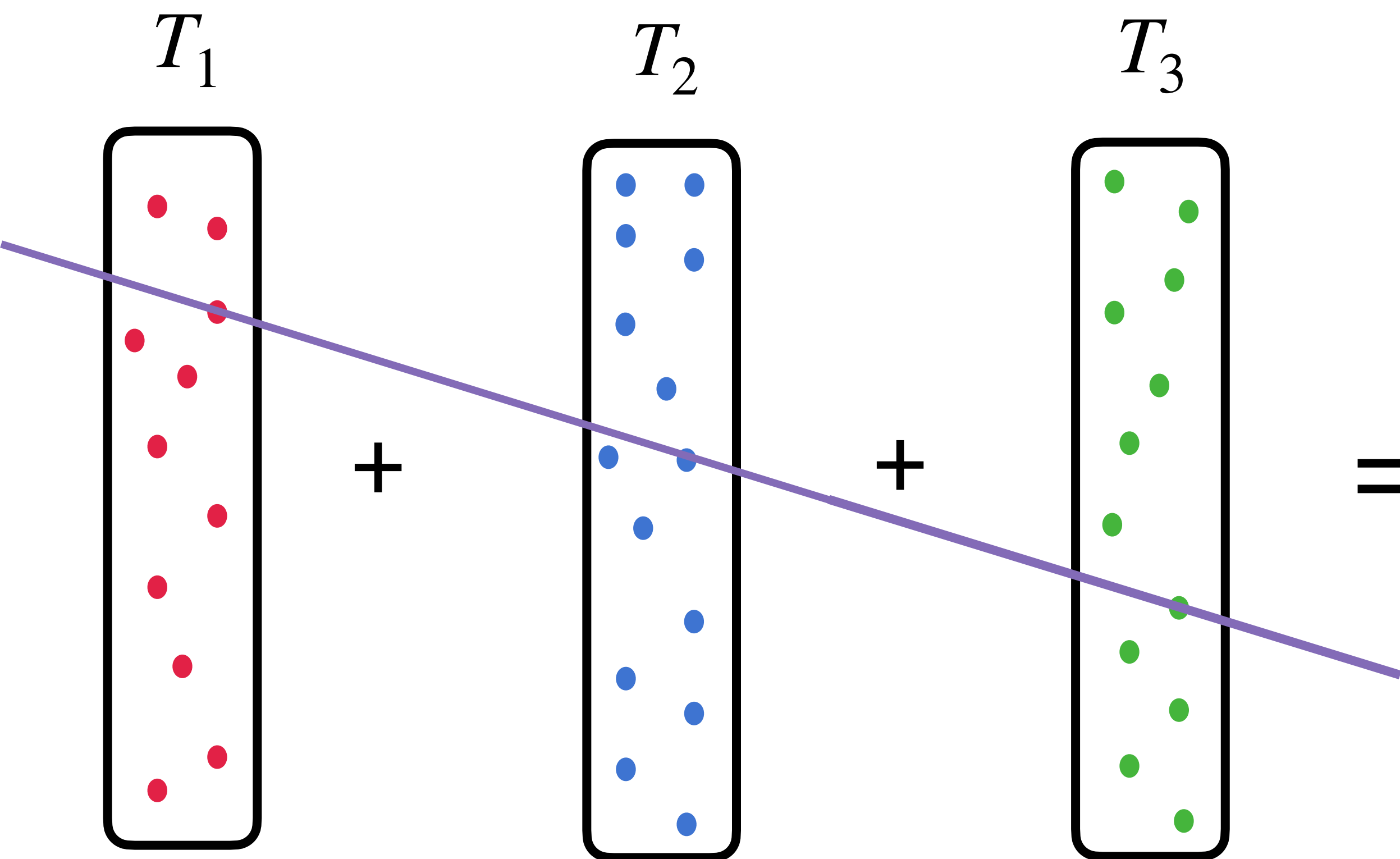
- Connections to Discrete Geometry, specifically SG-configurations.

$$C = \begin{array}{c} T_1 \\ \text{[red dots]} \end{array} + \begin{array}{c} T_2 \\ \text{[blue dots]} \end{array} + \begin{array}{c} T_3 \\ \text{[green dots]} \end{array} = 0$$

The diagram illustrates a cancellation in a sum. It shows three vertical rectangles, each containing a set of colored dots. The first rectangle, labeled T_1 , contains red dots. The second rectangle, labeled T_2 , contains blue dots. The third rectangle, labeled T_3 , contains green dots. These are arranged in a sum: $T_1 + T_2 + T_3 = 0$. A purple line is drawn diagonally across the plus sign between T_2 and T_3 , indicating that these two terms cancel each other out.

PIT for $\Sigma\Pi\Sigma(k)$ Circuits

- Connections to Discrete Geometry, specifically SG-configurations.

$$C = T_1 + T_2 + T_3 = 0$$


The diagram illustrates the equation $C = T_1 + T_2 + T_3 = 0$. Three vertical rectangles, labeled T_1 , T_2 , and T_3 from left to right, are shown. T_1 contains red dots, T_2 contains blue dots, and T_3 contains green dots. A purple line is drawn diagonally across the entire equation, crossing through all three rectangles.

PIT for $\Sigma\Pi\Sigma(k)$ Circuits

- Connections to Discrete Geometry, specifically SG-configurations.

$$C = \begin{array}{c} T_1 \\ \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \end{array} + \begin{array}{c} T_2 \\ \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \end{array} + \begin{array}{c} T_3 \\ \boxed{\begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \end{array}} \end{array} = 0$$

The diagram illustrates three sets of points, T_1 , T_2 , and T_3 , each enclosed in a rounded rectangular box. T_1 contains 8 red points, T_2 contains 8 blue points, and T_3 contains 8 green points. A purple line is drawn diagonally across the three boxes, intersecting the points in each set. The equation $C = T_1 + T_2 + T_3 = 0$ is shown, with the boxes containing the points acting as terms in the sum.

Coloured
High-Dimensional
Sylvester-Gallai!

PIT for $\Sigma\Pi\Sigma(k)$ Circuits

- Long-line of work [DS05, KS08, KS09, SS11, SS13] eventually give polytime Blackbox PIT when $k = \mathcal{O}(1)$.

PIT for $\Sigma\Pi\Sigma(k)$ Circuits

- Long-line of work [DS05, KS08, KS09, SS11, SS13] eventually give polytime Blackbox PIT when $k = \mathcal{O}(1)$.
- Identically zero $\Sigma\Pi\Sigma(k)$ circuits must be **low rank**.

$$\text{rank}(\text{sim}(C)) < 3k^2$$

Past Work on
Reconstruction of $\Sigma\Pi\Sigma(k)$
circuits

$$k = 1 \text{ or } 2$$

- $\Sigma\Pi\Sigma(1)$ circuits are just $\Pi\Sigma$ circuits. Factoring [Kal87]
- $\Sigma\Pi\Sigma(2)$ is already challenging, even though PIT is trivial because of Unique factorization.

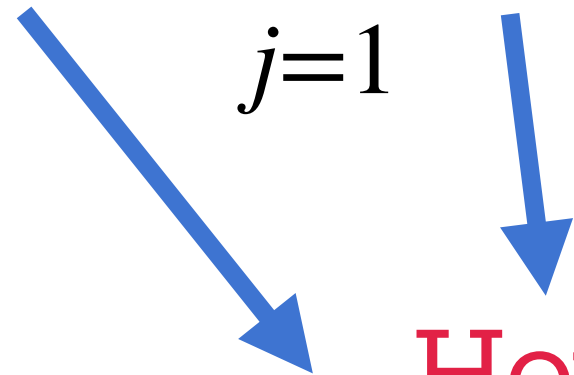
$$k = 1 \text{ or } 2$$

- $\Sigma\Pi\Sigma(1)$ circuits are just $\Pi\Sigma$ circuits. Factoring [Kal87]
- $\Sigma\Pi\Sigma(2)$ is already challenging, even though PIT is trivial because of Unique factorization.

$$C = \prod_{j=1}^d l_{1j} + \prod_{j=1}^d l_{2j}$$

$$k = 1 \text{ or } 2$$

- $\Sigma\Pi\Sigma(1)$ circuits are just $\Pi\Sigma$ circuits. Factoring [Kal87]
- $\Sigma\Pi\Sigma(2)$ is already challenging, even though PIT is trivial because of Unique factorization.

$$C = \prod_{j=1}^d l_{1j} + \prod_{j=1}^d l_{2j}$$


How do we learn these linear forms
From Blackbox access to C ?

Past Work

Results	Field	Model	Running Time
[Shp07]	\mathbb{F}_q	$\Sigma\Pi\Sigma(2)$	$\text{quasipoly}(n, d, \mathbb{F})$
[KS09]	\mathbb{F}_q	$\Sigma\Pi\Sigma(k), k = \mathcal{O}(1)$	$\text{quasipoly}(n, d, \mathbb{F})$
[Sin16]	$\mathbb{F} = \mathbb{R} \text{ or } \mathbb{C}$	$\Sigma\Pi\Sigma(2)$	$\text{poly}(n, d)$
[Sin22]	\mathbb{F}_q	$\Sigma\Pi\Sigma(2)$	$\text{poly}(n, d, \log \mathbb{F})$

Past Work

Results	Field	Model	Running Time
[Shp07]	\mathbb{F}_q	$\Sigma\Pi\Sigma(2)$	$\text{quasipoly}(n, d, \mathbb{F})$
[KS09]	\mathbb{F}_q	$\Sigma\Pi\Sigma(k), k = \mathcal{O}(1)$	$\text{quasipoly}(n, d, \mathbb{F})$
[Sin16]	$\mathbb{F} = \mathbb{R} \text{ or } \mathbb{C}$	$\Sigma\Pi\Sigma(2)$	$\text{poly}(n, d)$
[Sin22]	\mathbb{F}_q	$\Sigma\Pi\Sigma(2)$	$\text{poly}(n, d, \log \mathbb{F})$

In all of the above, it is Proper Learning only when rank is high.

Our Results

- $\mathbb{F} = \mathbb{R}$ or \mathbb{C} , $\Sigma\Pi\Sigma(3)$ circuits
- Randomized $(nd)^{\mathcal{O}(\log d)}$ time Reconstruction algorithm
- Proper learning when $\text{rank}(\text{sim}(T_i + T_j)) \geq c \log d$ for a constant c .

Our Results

- $\mathbb{F} = \mathbb{R}$ or \mathbb{C} , $\Sigma\Pi\Sigma(3)$ circuits
- Randomized $(nd)^{\mathcal{O}(\log d)}$ time Reconstruction algorithm
- Proper learning when $\text{rank}(\text{sim}(T_i + T_j)) \geq c \log d$ for a constant c .

First Subexponential Reconstruction Algorithm for $\Sigma\Pi\Sigma(3)$ circuits!

Proof Idea

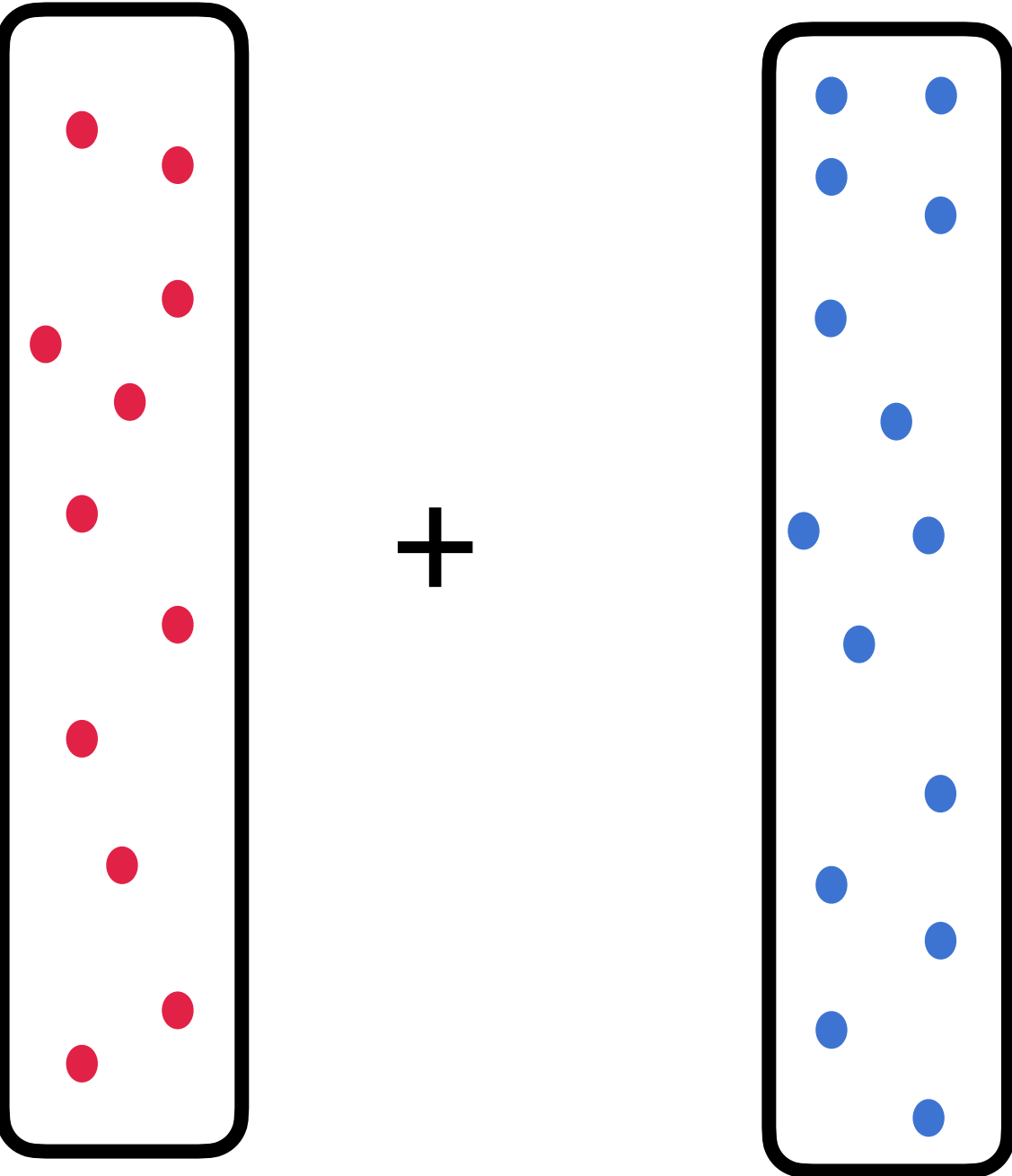
Proof Outline

- Prove Structural Results about $\Sigma\Pi\Sigma(3)$ circuits.
- Find few linear forms inside the circuit.
- Learn circuit from few linear forms.

Proof Outline

- Prove Structural Results about $\Sigma\Pi\Sigma(3)$ circuits.
- Find few linear forms inside the circuit.
- Learn circuit from few linear forms.

Learn Circuit from few linear forms[Shp07, KS09]

$$C = T_1 + T_2 = \prod_{j=1}^d l_{2j}$$


The diagram illustrates the decomposition of a circuit C into two parts, T_1 and T_2 . T_1 is represented by a vertical rectangle containing 10 red dots. T_2 is represented by a vertical rectangle containing 10 blue dots. The two rectangles are separated by a plus sign, indicating their sum.

Learn Circuit from few linear forms[Shp07, KS09]

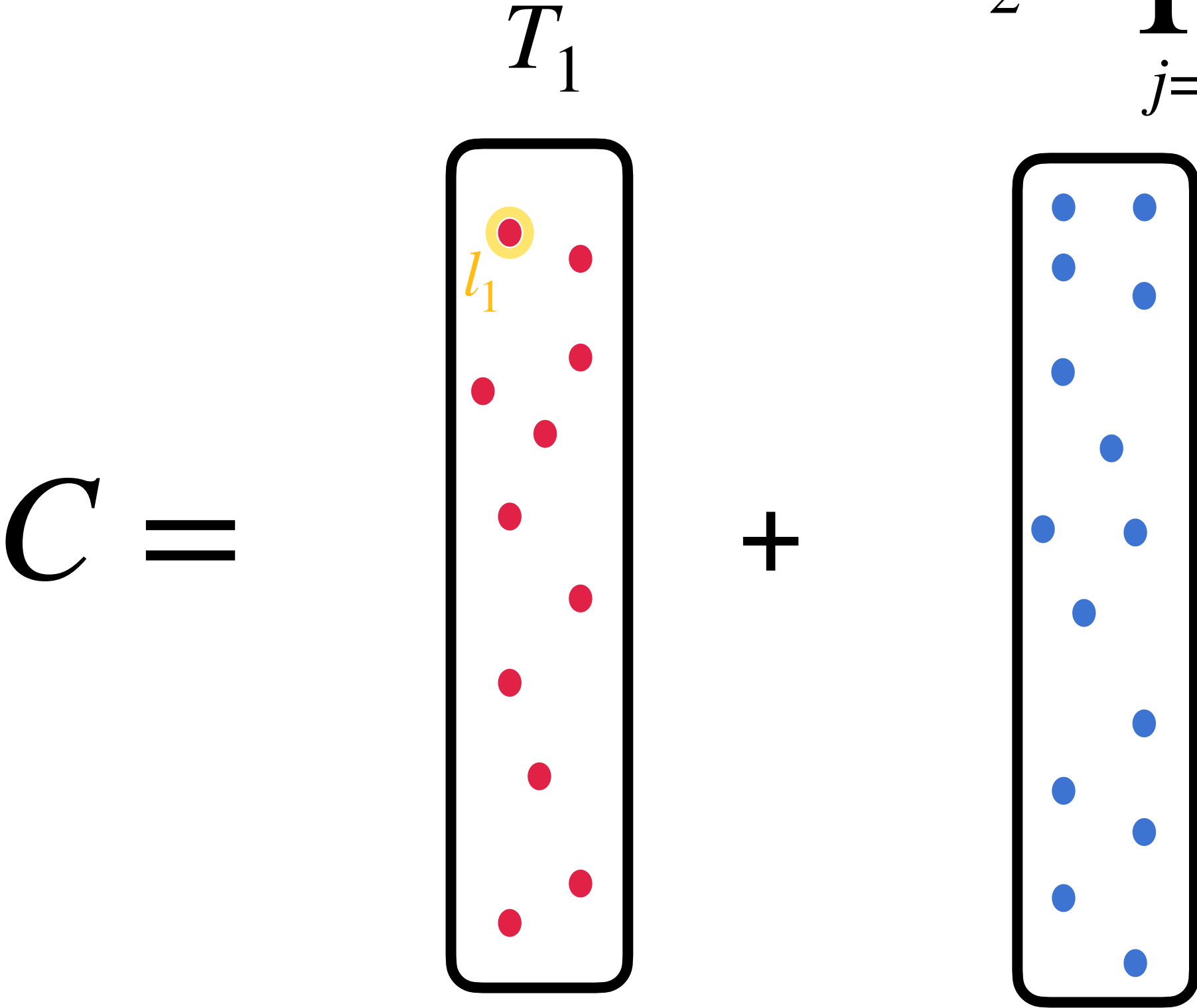
$$C = T_1 + T_2 = \prod_{j=1}^d l_{2j} \quad C \bmod l_1$$

The diagram illustrates the decomposition of a circuit C into two parts, T_1 and T_2 . T_1 is represented by a vertical rectangle containing 10 red dots, with the top dot highlighted in yellow and labeled l_1 . T_2 is represented by a vertical rectangle containing 10 blue dots. The equation $C = T_1 + T_2$ is shown, followed by the product formula for T_2 and the modulo operation for C .

Learn Circuit from few linear forms[Shp07, KS09]

$$C \bmod l_1 = T_2 \bmod l_1$$

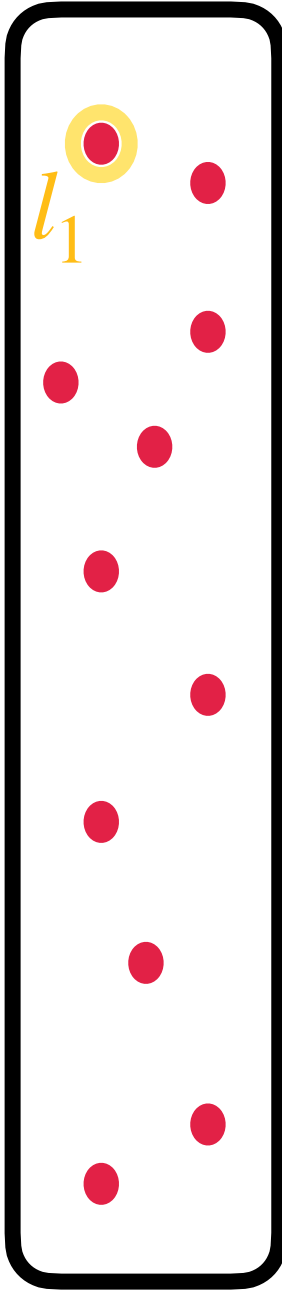
$$T_2 = \prod_{j=1}^d l_{2j}$$



Learn Circuit from few linear forms[Shp07, KS09]

$C =$

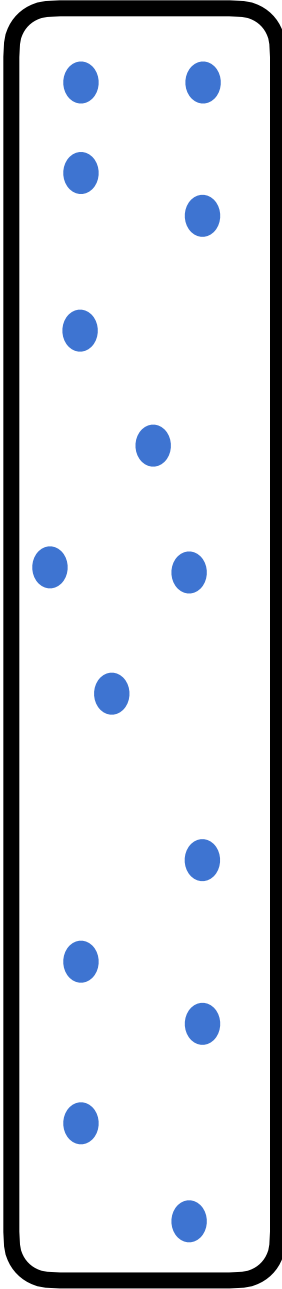
T_1



l_1

$+$

$T_2 = \prod_{j=1}^d l_{2j}$



Learn Circuit from few linear forms[Shp07, KS09]

$$C = T_1 + T_2 \bmod l_1$$

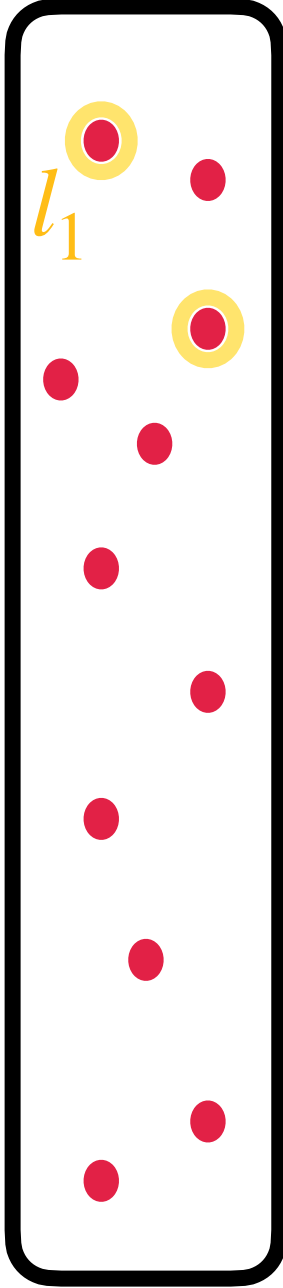
$T_2 = \prod_{j=1}^d l_{2j}$

The diagram illustrates the decomposition of a circuit C into two parts, T_1 and T_2 , modulo l_1 . On the left, the expression $C =$ is followed by a vertical rectangle containing 12 red dots. The top dot in this rectangle is highlighted with a yellow circle and labeled l_1 . To the right of this rectangle is a plus sign $+$, followed by another vertical rectangle containing 12 blue dots. To the right of the blue rectangle is the expression $T_2 \bmod l_1$. Above the blue rectangle, the formula $T_2 = \prod_{j=1}^d l_{2j}$ is written.

Learn Circuit from few linear forms[Shp07, KS09]

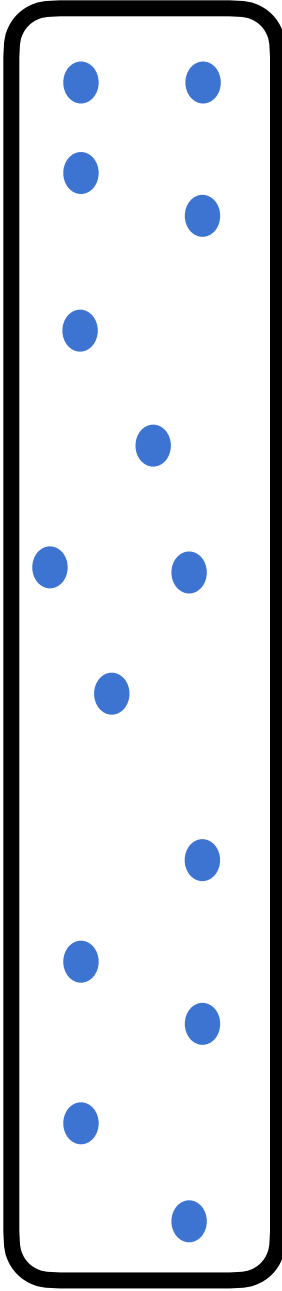
$C =$

T_1



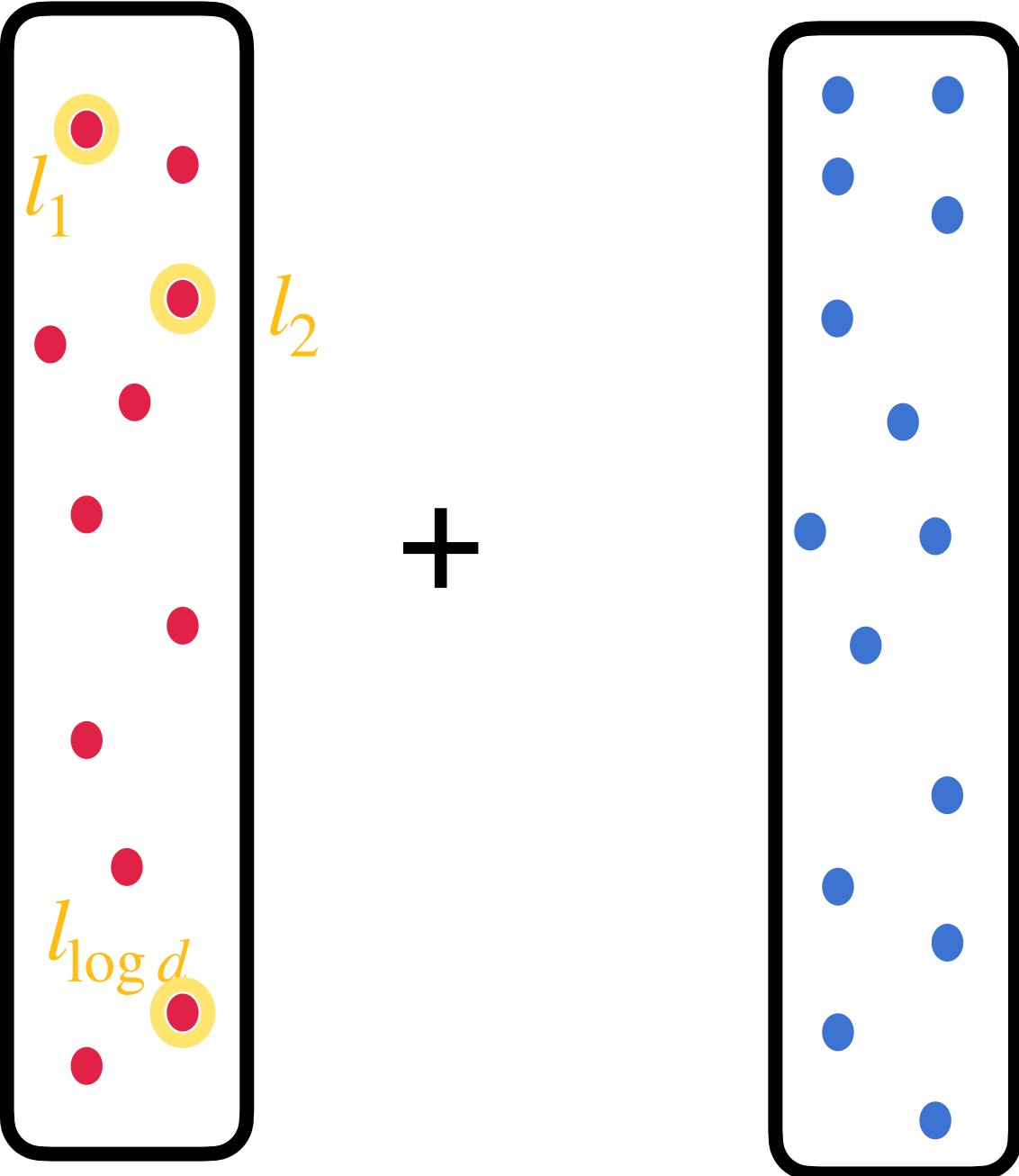
$+$

$T_2 = \prod_{j=1}^d l_{2j}$



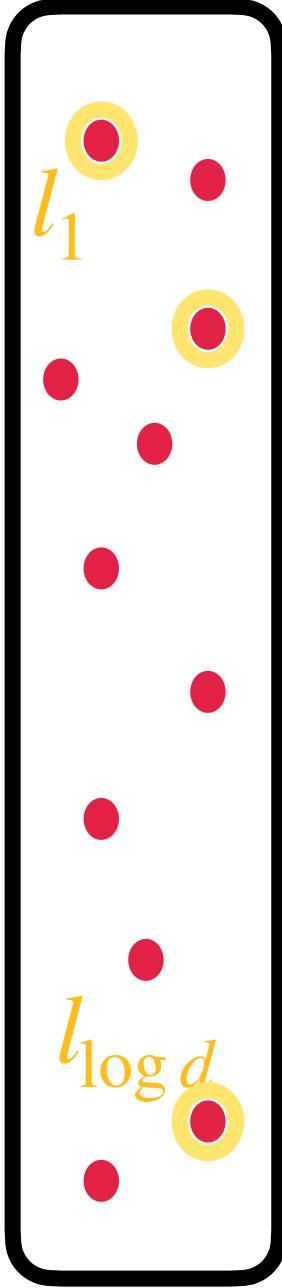
$T_2 \bmod l_1$

Learn Circuit from few linear forms[Shp07, KS09]

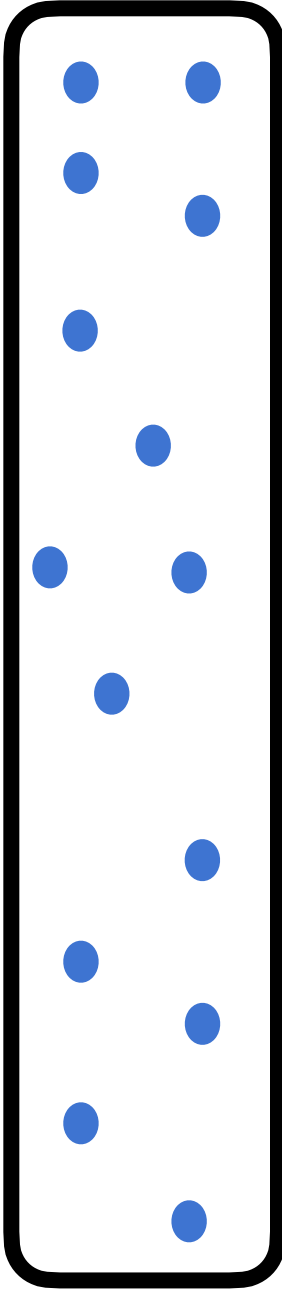
$$C = \begin{matrix} T_1 \\ \begin{array}{|c|} \hline \text{Red dots} \\ \hline \end{array} \\ + \\ \begin{matrix} T_2 = \prod_{j=1}^d l_{2j} \\ \begin{array}{|c|} \hline \text{Blue dots} \\ \hline \end{array} \end{matrix} \pmod{l_1}$$


Learn Circuit from few linear forms[Shp07, KS09]

$C =$

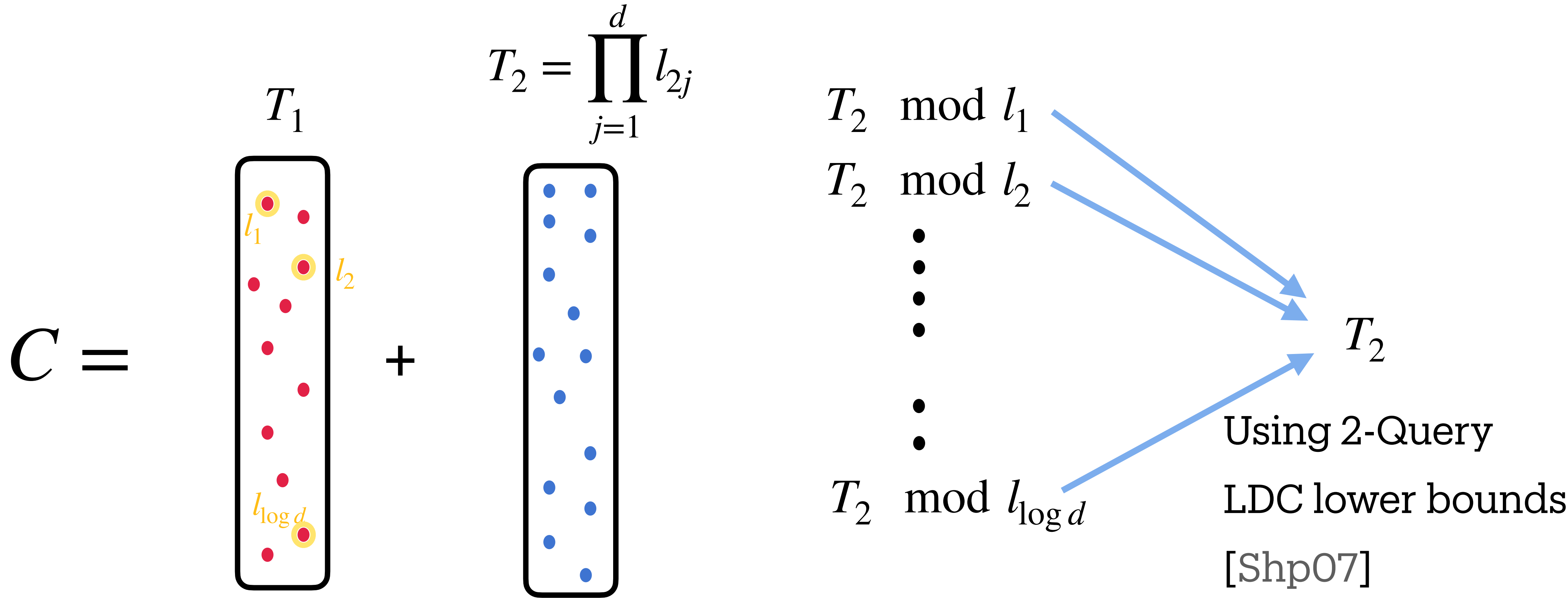
T_1
 l_1 l_2 $l_{\log d}$

$+$

$T_2 = \prod_{j=1}^d l_{2j}$


$T_2 \bmod l_1$
 $T_2 \bmod l_2$
 \vdots
 $T_2 \bmod l_{\log d}$

Learn Circuit from few linear forms[Shp07, KS09]



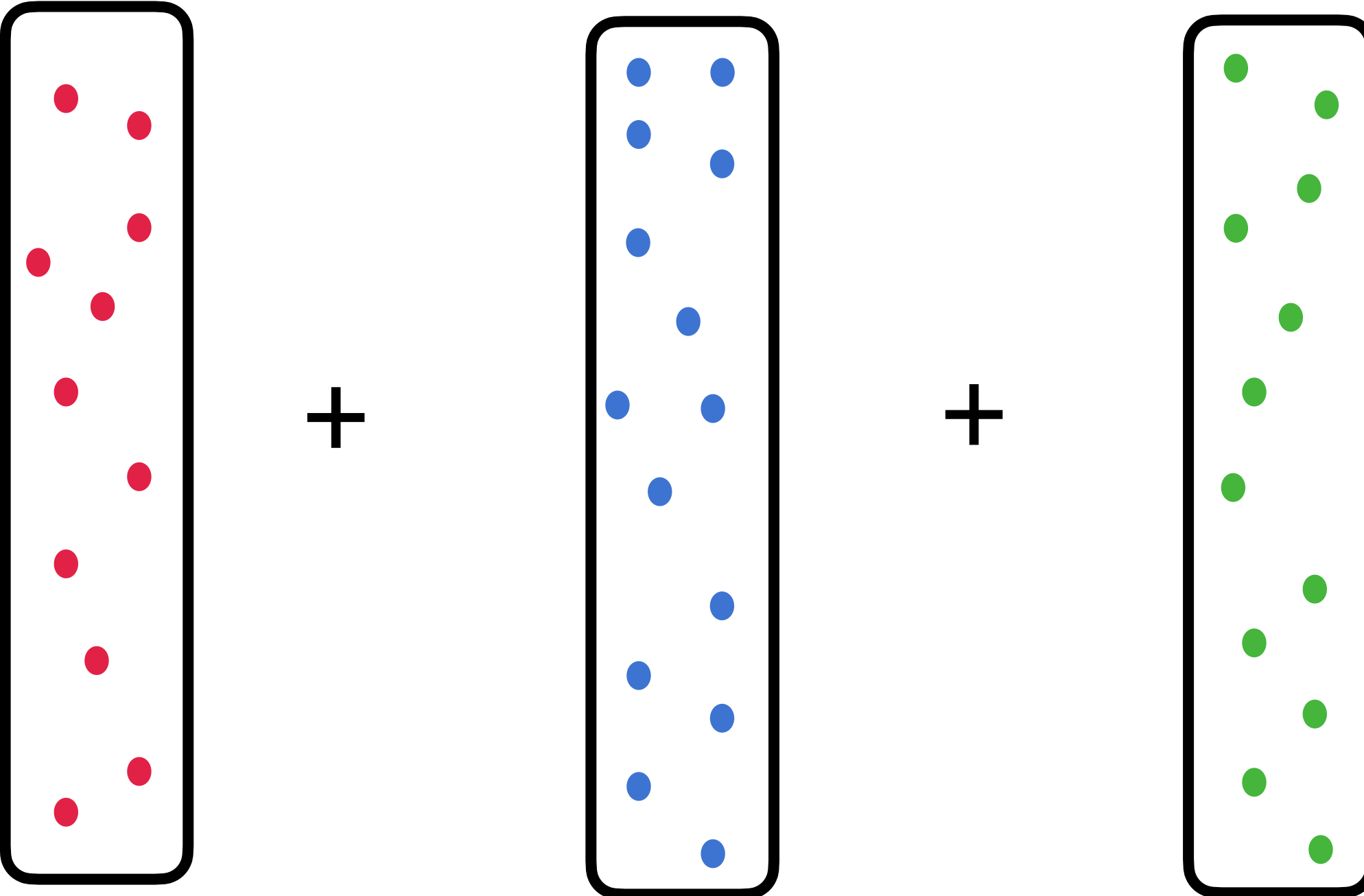
Learn Circuit from few linear forms[Shp07, KS09]

- [KS09] generalized this technique to work for projections of $\Sigma\Pi\Sigma(k)$ circuits.

Learn Circuit from few linear forms[Shp07, KS09]

- [KS09] generalized this technique to work for projections of $\Sigma\Pi\Sigma(k)$ circuits.
- Where do we get the linear forms?
- [Shp07, KS09] Find a variable reduction to $\log d$ variables, and brute force over all linear forms in \mathbb{F} over $\log d$ variables.
- Can't do it for \mathbb{R} or \mathbb{C}

Vanishing Spaces

$$C = T_1 + T_2 + T_3$$


The diagram illustrates the decomposition of a space C into three subspaces T_1 , T_2 , and T_3 . Each subspace is represented by a vertical rounded rectangle containing a set of colored dots. T_1 contains 12 red dots, T_2 contains 12 blue dots, and T_3 contains 12 green dots. The subspaces are summed together to form C .

Subspace	Color	Count
T_1	Red	12
T_2	Blue	12
T_3	Green	12

Vanishing Spaces

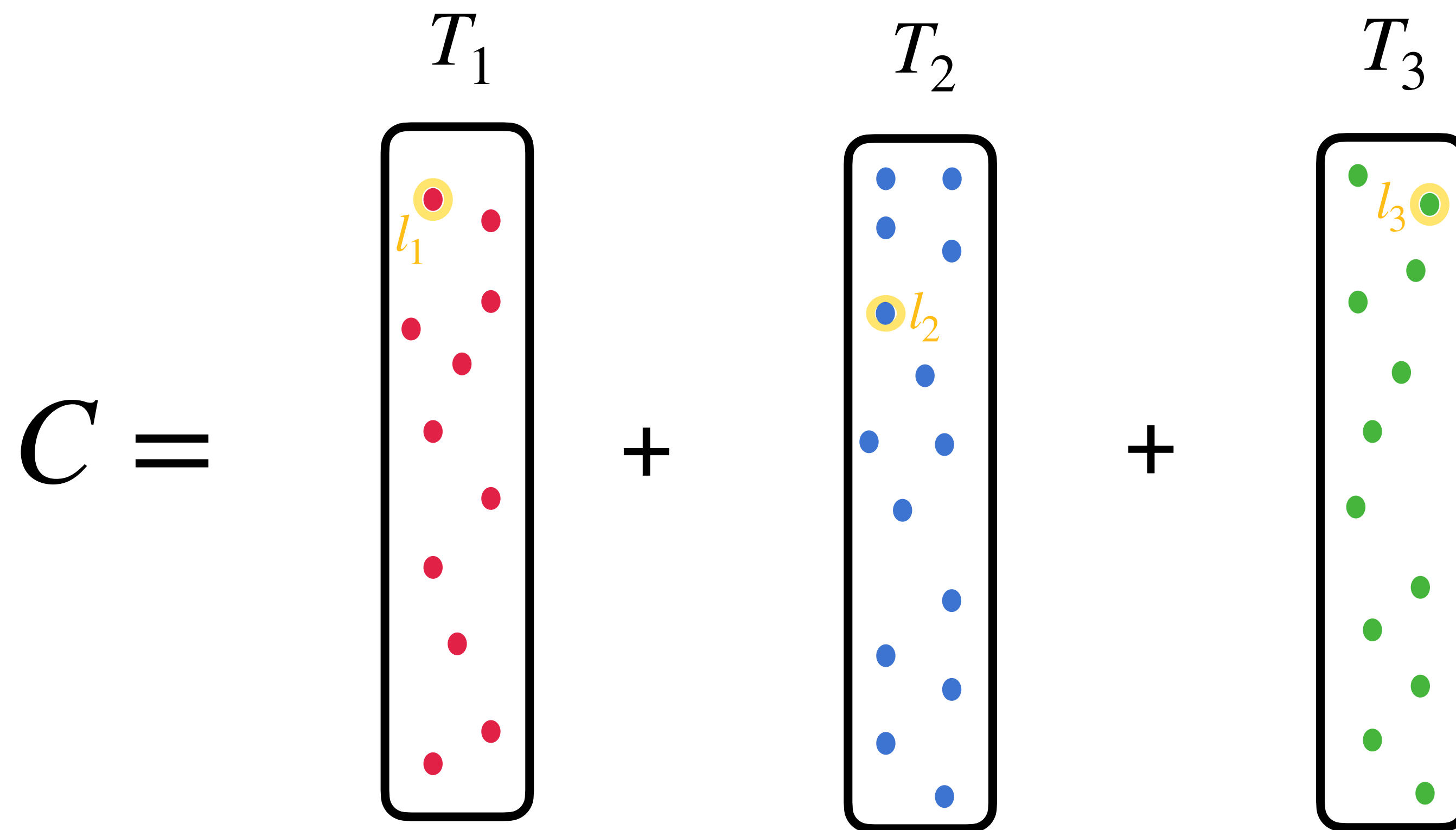
$$C = T_1 + T_2 + T_3$$

The diagram illustrates the decomposition of a space C into three components T_1 , T_2 , and T_3 . Each component is represented by a vertical rectangle containing a set of colored dots. The dots in T_1 are red, in T_2 are blue, and in T_3 are green. A yellow circle highlights a specific dot in each rectangle, labeled l_1 , l_2 , and l_3 respectively. The equation $C = T_1 + T_2 + T_3$ is shown to the left of the rectangles.

Vanishing Spaces

$$C \bmod \langle l_1, l_2, l_3 \rangle = 0$$

$$\mathbb{V}(l_1, l_2, l_3)$$



Vanishing Spaces

$$C = T_1 + T_2 + T_3 \quad \mathbb{V}(l_1, l_2, l_3)$$

The diagram illustrates the decomposition of a space C into three components T_1 , T_2 , and T_3 , which are summed together. Each component is represented by a vertical rectangle containing a set of points. The points in T_1 are red, in T_2 are blue, and in T_3 are green. A specific point in each set is highlighted with a yellow circle and labeled l_1 , l_2 , and l_3 respectively. The labels l_1 , l_2 , and l_3 are written in yellow. The entire expression is followed by the notation $\mathbb{V}(l_1, l_2, l_3)$.

Vanishing Spaces

$$C = T_1 + T_2 + T_3 \quad \mathbb{V}(l_1, l_2, l_3)$$

The diagram illustrates the decomposition of a space C into three components T_1 , T_2 , and T_3 . Each component is represented by a vertical rectangle containing points of a specific color. T_1 contains red points, T_2 contains blue points, and T_3 contains green points. A yellow circle highlights a specific point in each rectangle, labeled l_1 , l_2 , and l'_3 respectively. The labels l_1 , l_2 , and l'_3 are placed next to their respective highlighted points. The entire expression is followed by the notation $\mathbb{V}(l_1, l_2, l_3)$.

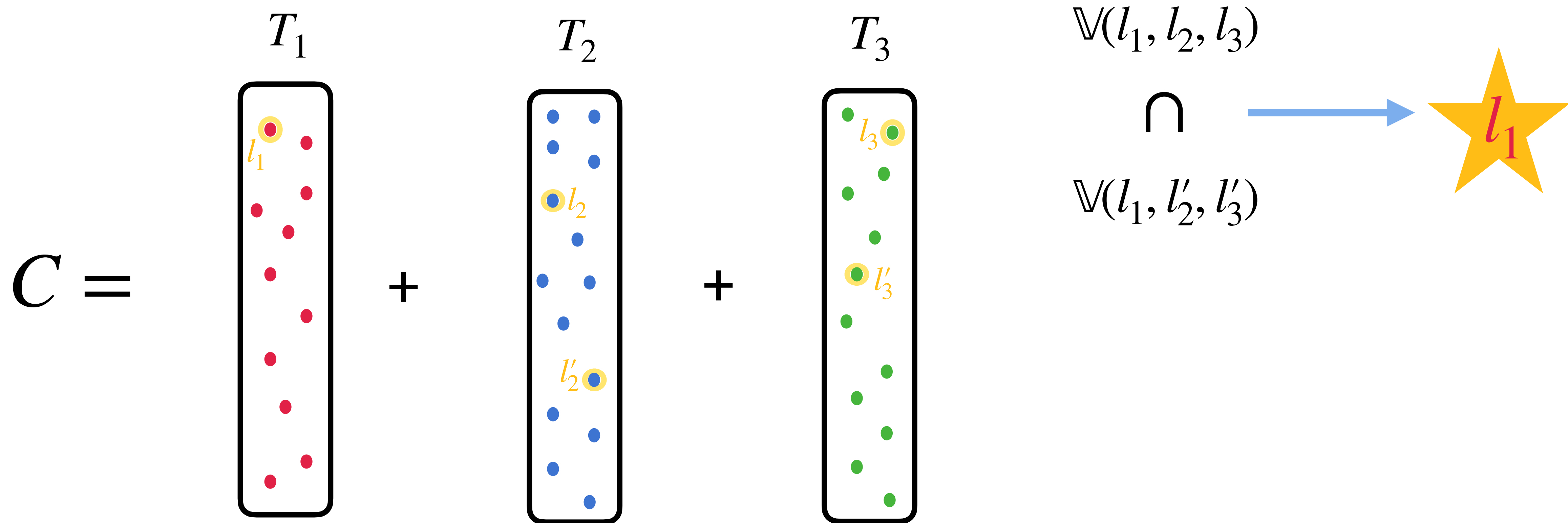
Vanishing Spaces

$$C = T_1 + T_2 + T_3 \quad \mathbb{V}(l_1, l_2, l_3)$$

$$\mathbb{V}(l_1, l'_2, l'_3)$$

The diagram illustrates the decomposition of a curve C into three components T_1 , T_2 , and T_3 . Each component is represented by a vertical rectangle containing several points. T_1 contains red points, T_2 contains blue points, and T_3 contains green points. The points l_1 , l_2 , and l_3 are highlighted in yellow in T_1 , T_2 , and T_3 respectively. The points l'_1 , l'_2 , and l'_3 are also highlighted in yellow in T_1 , T_2 , and T_3 respectively. The vanishing spaces $\mathbb{V}(l_1, l_2, l_3)$ and $\mathbb{V}(l_1, l'_2, l'_3)$ are indicated to the right of the components.

Vanishing Spaces



Vanishing Spaces

- \mathcal{S}_3 be the set of co-dimension 3 vanishing spaces.
- Is \mathcal{S}_3 finite?

$$C = \begin{array}{c} T_1 \\ \text{[red dots]} \end{array} + \begin{array}{c} T_2 \\ \text{[blue dots]} \end{array} + \begin{array}{c} T_3 \\ \text{[green dots]} \end{array}$$

Vanishing Spaces

- \mathcal{S}_3 be the set of co-dimension 3 vanishing spaces.
- Is \mathcal{S}_3 finite?

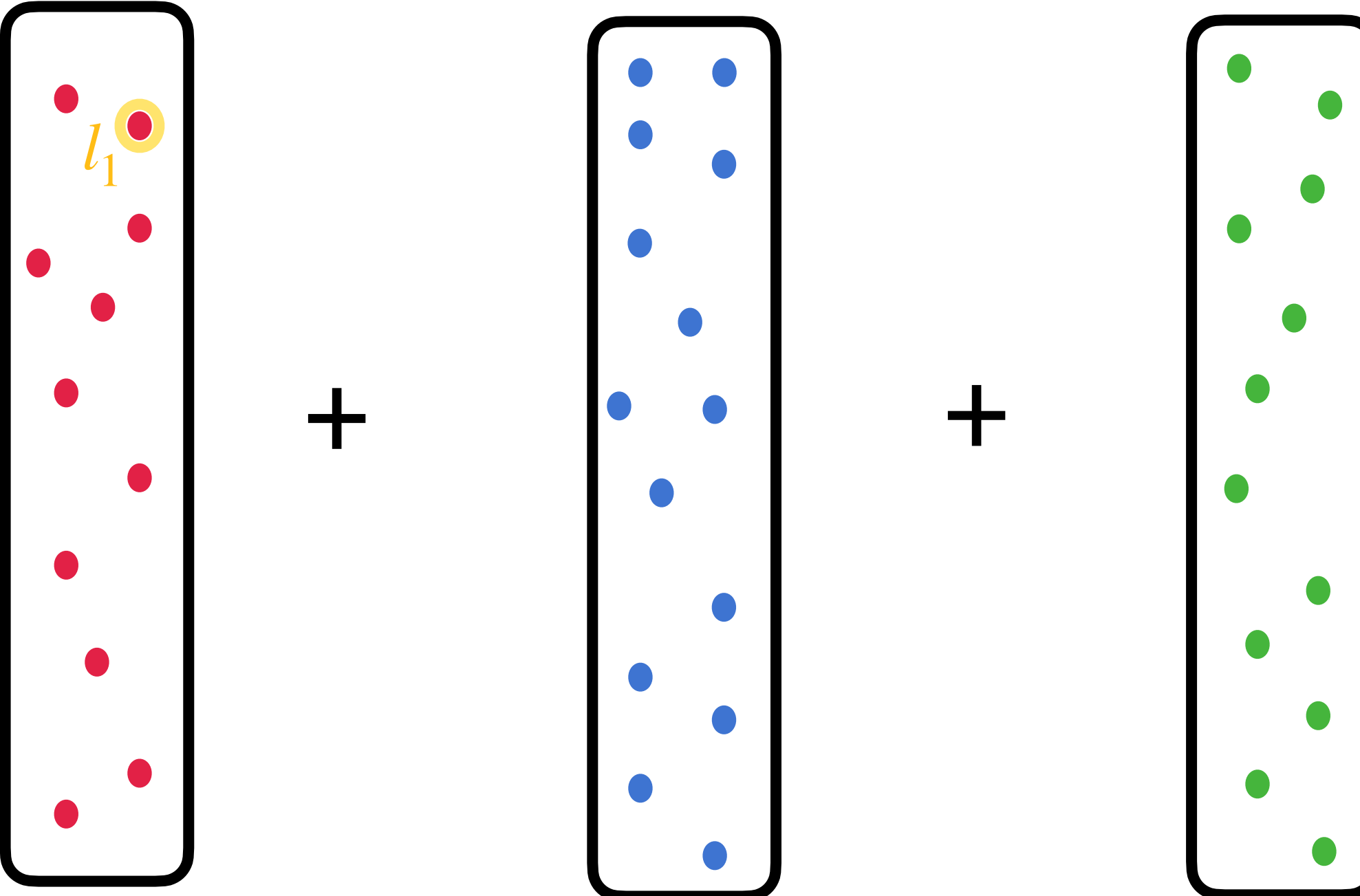
$$C = T_1 + T_2 + T_3$$

The diagram illustrates the addition of three vanishing spaces T_1 , T_2 , and T_3 to form C . Each space is represented by a vertical rectangle containing points. T_1 contains 10 red points, with one point highlighted by a yellow circle and labeled l_1 . T_2 contains 10 blue points, with one point highlighted by a yellow circle and labeled l_2 . T_3 contains 10 green points, with one point highlighted by a purple circle and labeled $l_1 + l_2$. The diagram shows the union of these sets, with the label $l_1 + l_2$ appearing below the third rectangle.

$$\mathbb{V}(l_1, l_2, *)$$

Vanishing Spaces

- \mathcal{S}_3 be the set of co-dimension 3 vanishing spaces.
- Is \mathcal{S}_3 finite?

$$C = T_1 + T_2 + T_3$$


The diagram illustrates the decomposition of a set C into three vanishing spaces T_1 , T_2 , and T_3 . Each space is represented by a vertical rectangle containing points of a specific color: red for T_1 , blue for T_2 , and green for T_3 . The spaces are separated by plus signs, indicating their union. A yellow circle labeled l_1 is highlighted within T_1 .

Vanishing Spaces

- \mathcal{S}_3 be the set of co-dimension 3 vanishing spaces.
- Is \mathcal{S}_3 finite?

$$C = T_1 + T_2 + T_3 \quad \mathbb{V}(l_1, *, *)$$

The diagram illustrates the decomposition of a curve C into three components T_1 , T_2 , and T_3 . Each component is represented by a vertical rectangle containing points of a specific color. T_1 contains 10 red points, with one point highlighted in yellow and labeled l_1 . T_2 contains 14 blue points, with one point highlighted in yellow and labeled $2l_1$. T_3 contains 12 green points, with one point highlighted in yellow and labeled $5l_1$. The components are summed to form C , which is associated with the vanishing space $\mathbb{V}(l_1, *, *)$.

Vanishing Spaces

\mathcal{S}_1

Codimension 1 spaces

\mathcal{S}_2

Codimension 2 spaces

not contained in \mathcal{S}_1

\mathcal{S}_3

Codimension 3 spaces

not contained in \mathcal{S}_1 and \mathcal{S}_2

Vanishing Spaces

\mathcal{S}_1

Codimension 1 spaces

\mathcal{S}_2

Codimension 2 spaces

not contained in \mathcal{S}_1

\mathcal{S}_3

Codimension 3 spaces

not contained in \mathcal{S}_1 and \mathcal{S}_2

Are the only spaces where all T_1, T_2, T_3 vanish?

Example

$$(x_1 + x_3)(x_2 - x_3)(x_4 + x_2) + (x_1 + x_2 - x_3)(x_2 + 5x_3)(x_5 + 4x_3) + (x_1 + 2x_2 - 3x_3)(5x_3 - 3x_2)(x_4 + 7x_5 + 15x_2)$$

Example

$$(x_1 + x_3)(x_2 - x_3)(x_4 + x_2) + (x_1 + x_2 - x_3)(x_2 + 5x_3)(x_5 + 4x_3) + (x_1 + 2x_2 - 3x_3)(5x_3 - 3x_2)(x_4 + 7x_5 + 15x_2)$$

Go mod $(x_2 - 2x_3)$

Example

$$(x_1 + x_3)(x_2 - x_3)(x_4 + x_2) + (x_1 + x_2 - x_3)(x_2 + 5x_3)(x_5 + 4x_3) + (x_1 + 2x_2 - 3x_3)(5x_3 - 3x_2)(x_4 + 7x_5 + 15x_2)$$

Go mod $(x_2 - 2x_3)$

$$(x_1 + x_3)(x_3)(x_4 + 2x_3) + (x_1 + x_3)(7x_3)(x_5 + 4x_3) + (x_1 + x_3)(-x_3)(x_4 + 7x_5 + 30x_3) = 0$$

Proof Outline

Steps

- Showing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have size $d^{\mathcal{O}(1)}$ when C has high rank.

Proof Outline

Steps

- Showing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have size $d^{\mathcal{O}(1)}$ when C has high rank.
- Computing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have in $\text{poly}(n, d)$ time.

Proof Outline

Steps

- Showing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have size $d^{\mathcal{O}(1)}$ when C has high rank.
- Computing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have in $\text{poly}(n, d)$ time.
- Learning $\mathcal{O}(\log d)$ linear forms from a gate using $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$.

Proof Outline

Steps

- Showing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have size $d^{\mathcal{O}(1)}$ when C has high rank.
- Computing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have in $\text{poly}(n, d)$ time.
- Learning $\mathcal{O}(\log d)$ linear forms from a gate using $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$.
- Using techniques from [Shp07, KS09] to reconstruct the circuit.

Proof Outline

Steps

- Showing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have size $d^{\mathcal{O}(1)}$ when C has high rank.
- Computing $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ have in $\text{poly}(n, d)$ time.
- Learning $\mathcal{O}(\log d)$ linear forms from a gate using $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$.
- Using techniques from [Shp07, KS09] to reconstruct the circuit.

Bounding \mathcal{S}_1

$$C \bmod l = 0$$

Bounding \mathcal{S}_1

$$C \bmod l = 0 \longrightarrow l \mid C$$

Bounding \mathcal{S}_1

$$C \bmod l = 0 \quad \longrightarrow \quad l \mid C$$

- Degree d polynomial has at most d factors.

$$|\mathcal{S}_1| \leq d$$

Bounding \mathcal{S}_1

$$C \bmod l = 0 \quad \longrightarrow \quad l \mid C$$

- Degree d polynomial has at most d factors.

$$|\mathcal{S}_1| \leq d$$

Theorem[DS06, Shp07, KS09]

Let $\mathcal{L} := \{l : l \mid \text{sim}(C)\}$. Then $\dim(\text{span}(\mathcal{L})) = \mathcal{O}(\log d)$

Bounding \mathcal{S}_1

$$C \bmod l = 0 \quad \longrightarrow \quad l \mid C$$

- Degree d polynomial has at most d factors.

$$|\mathcal{S}_1| \leq d$$

Theorem[DS06, Shp07, KS09]

Let $\mathcal{L} := \{l : l \mid \text{sim}(C)\}$. Then $\dim(\text{span}(\mathcal{L})) = \mathcal{O}(\log d)$

From 2-Query LDC
Lower bounds

Bounding \mathcal{S}_2

- Consider $\mathbb{V}(l_1, l_2) \in \mathcal{S}_2$.
- **EASY CASE:** When some T_i vanishes on $\mathbb{V}(l_1, l_2)$.

Bounding \mathcal{S}_2

- Consider $\mathbb{V}(l_1, l_2) \in \mathcal{S}_2$.
- **EASY CASE:** When some T_i vanishes on $\mathbb{V}(l_1, l_2)$.

$$l \mid T_1 \text{ and } l \in \text{span}(l_1, l_2)$$

Bounding \mathcal{S}_2

- Consider $\mathbb{V}(l_1, l_2) \in \mathcal{S}_2$.
- **EASY CASE:** When some T_i vanishes on $\mathbb{V}(l_1, l_2)$.

$$l \mid T_1 \text{ and } l \in \text{span}(l_1, l_2)$$

$$\text{span}(l, l') = \text{span}(l_1, l_2)$$

Bounding \mathcal{S}_2

- Consider $\mathbb{V}(l_1, l_2) \in \mathcal{S}_2$.
- **EASY CASE:** When some T_i vanishes on $\mathbb{V}(l_1, l_2)$.

$$l \mid T_1 \text{ and } l \in \text{span}(l_1, l_2)$$

$$C \bmod l \neq 0$$

$$\text{span}(l, l') = \text{span}(l_1, l_2)$$

Bounding \mathcal{S}_2

- Consider $\mathbb{V}(l_1, l_2) \in \mathcal{S}_2$.
- **EASY CASE:** When some T_i vanishes on $\mathbb{V}(l_1, l_2)$.

$$l \mid T_1 \text{ and } l \in \text{span}(l_1, l_2)$$

$$C \bmod l \neq 0$$

$$l' \mid (C \bmod l)$$

$$\text{span}(l, l') = \text{span}(l_1, l_2)$$

Bounding \mathcal{S}_2

- Consider $\mathbb{V}(l_1, l_2) \in \mathcal{S}_2$.
- **EASY CASE:** When some T_i vanishes on $\mathbb{V}(l_1, l_2)$.

$$l \mid T_1 \text{ and } l \in \text{span}(l_1, l_2)$$

$$C \bmod l \neq 0$$

$$l' \mid (C \bmod l)$$

$$\text{span}(l, l') = \text{span}(l_1, l_2)$$

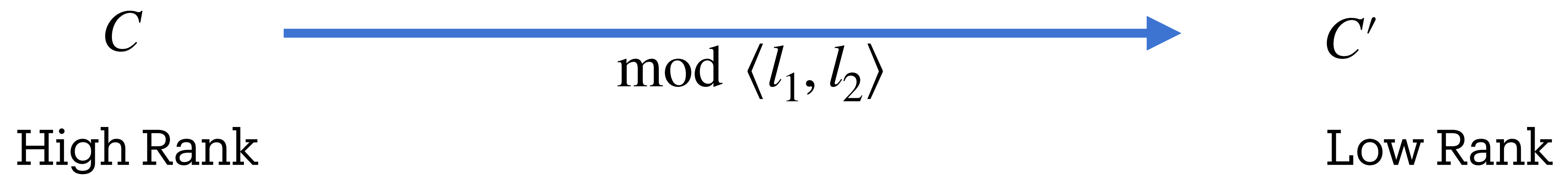
Possibilities for $\mathbb{V}(l_1, l_2)$ at most d^2

Bounding \mathcal{S}_2

- When No gate vanishes on $\mathbb{V}(l_1, l_2)$:

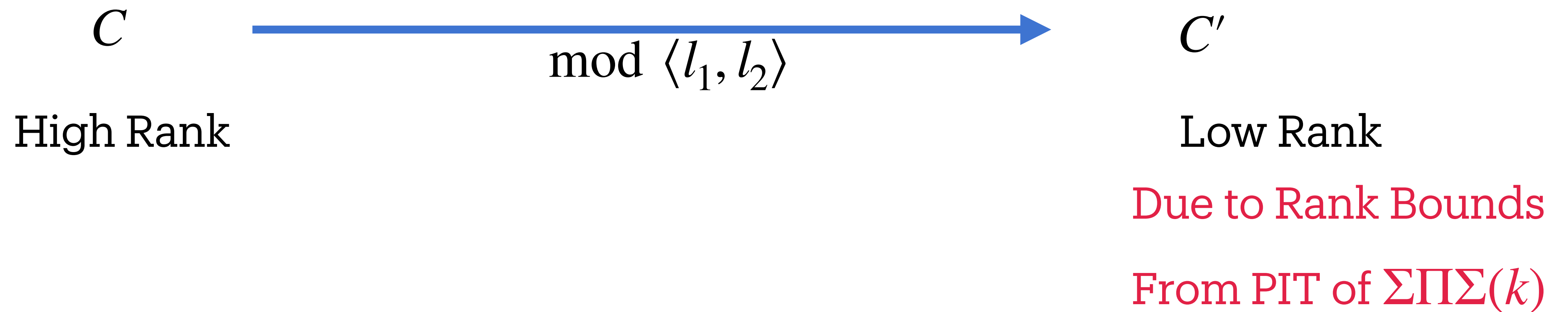
Bounding \mathcal{S}_2

- When No gate vanishes on $\mathbb{V}(l_1, l_2)$:



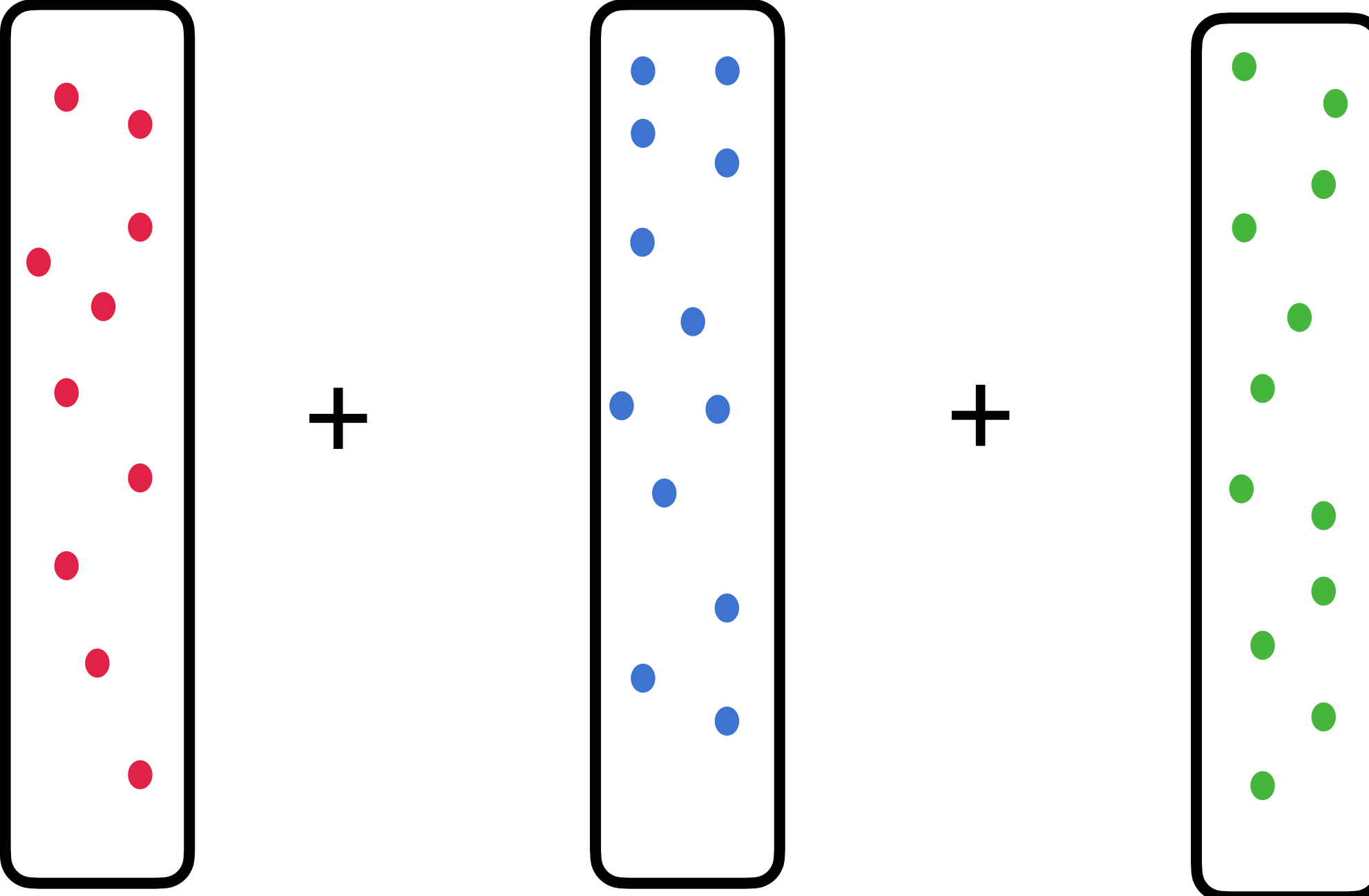
Bounding \mathcal{S}_2

- When No gate vanishes on $\mathbb{V}(l_1, l_2)$:



Bounding \mathcal{S}_2

High Rank

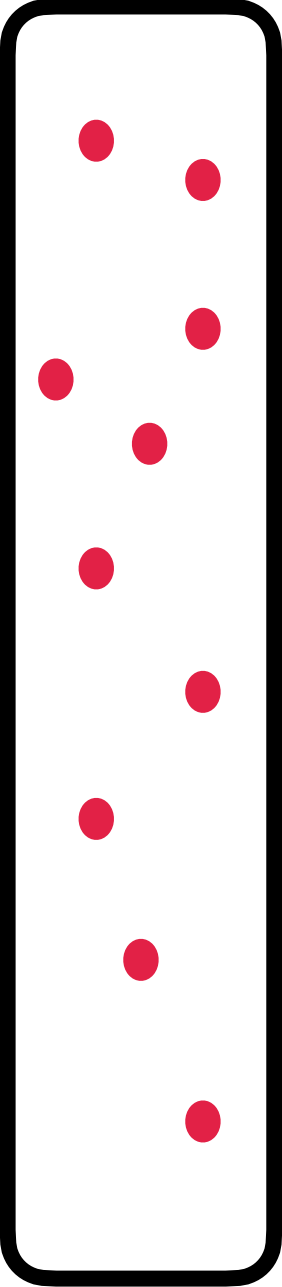
$$C = T_1 + T_2 + T_3$$


The diagram illustrates the decomposition of a matrix C into three components: T_1 , T_2 , and T_3 . Each component is represented by a vertical rounded rectangle containing a set of colored dots. T_1 contains 12 red dots, T_2 contains 12 blue dots, and T_3 contains 12 green dots. The components are summed together to equal C .

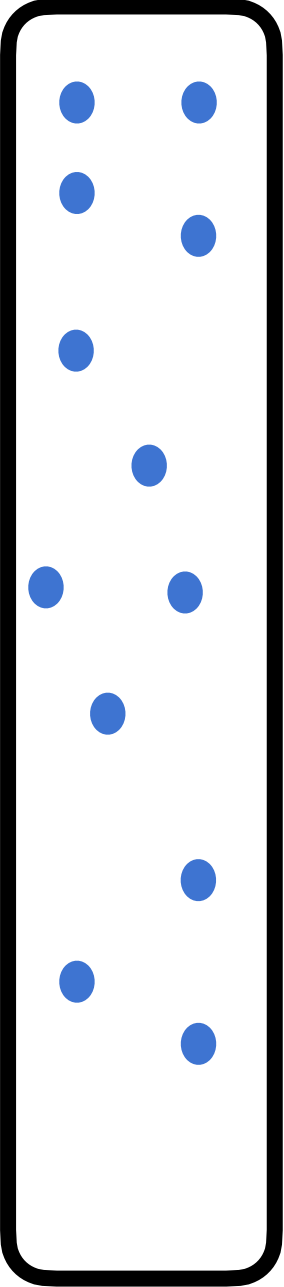
Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

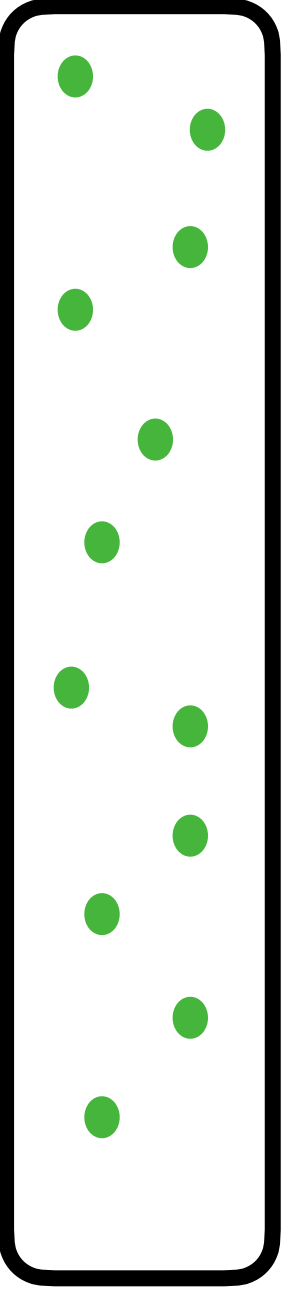
$C =$

T_1 

+

T_2 

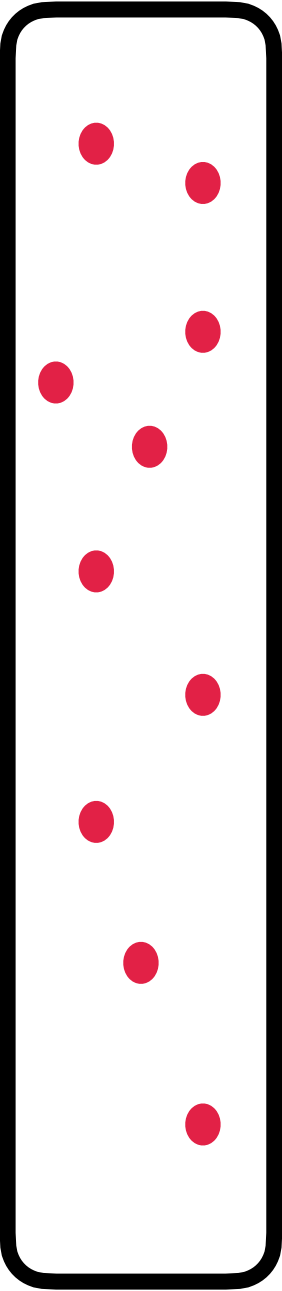
+

T_3 

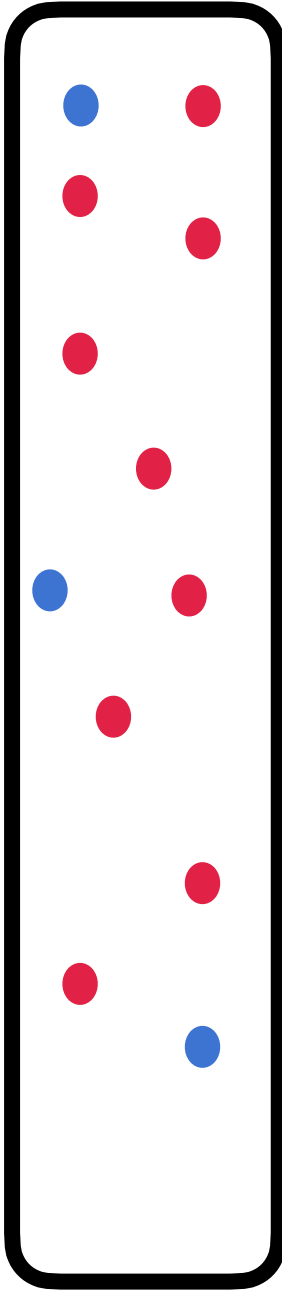
Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

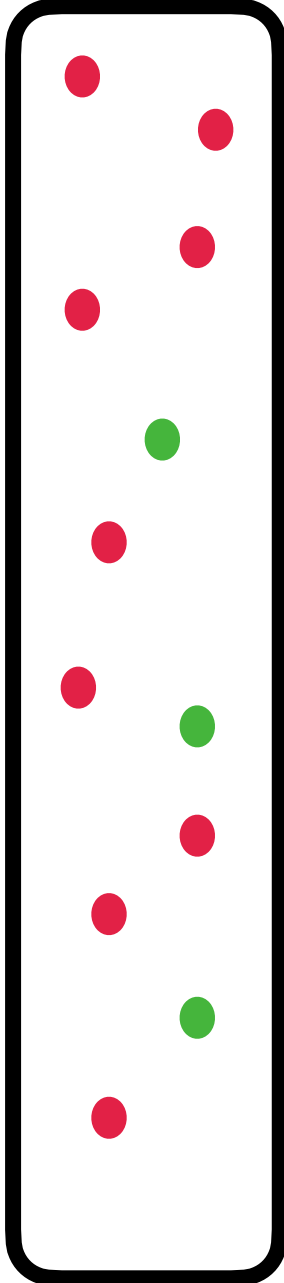
$$C =$$

T_1 

+

T_2 

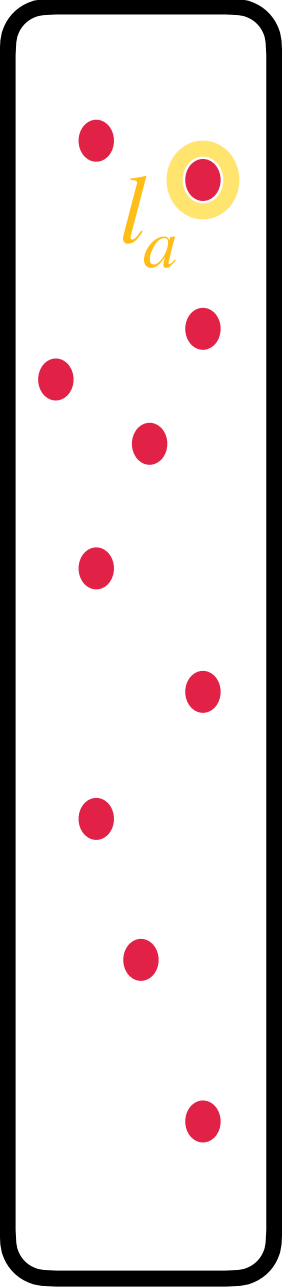
+

T_3 

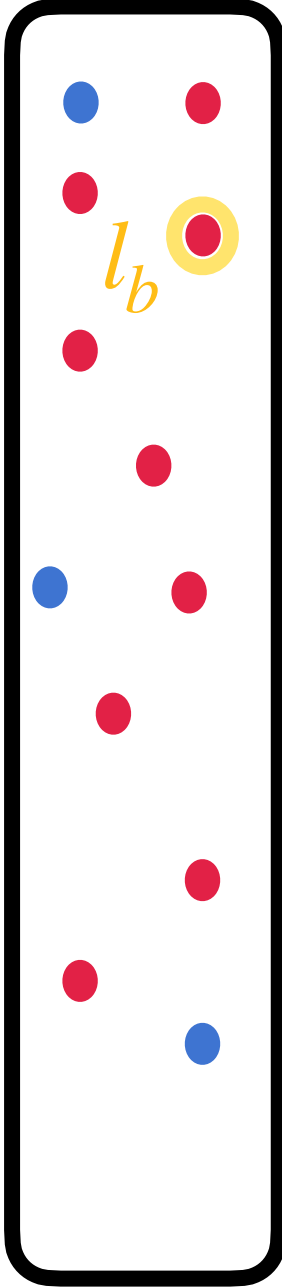
Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

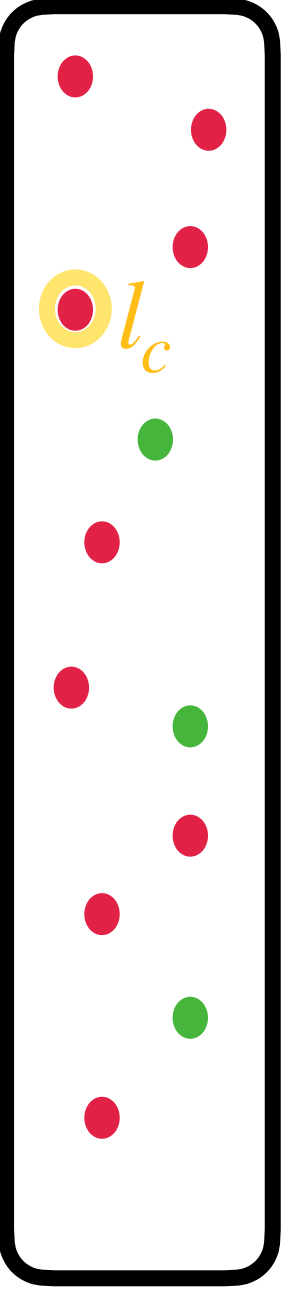
$C =$

T_1 

+

T_2 

+

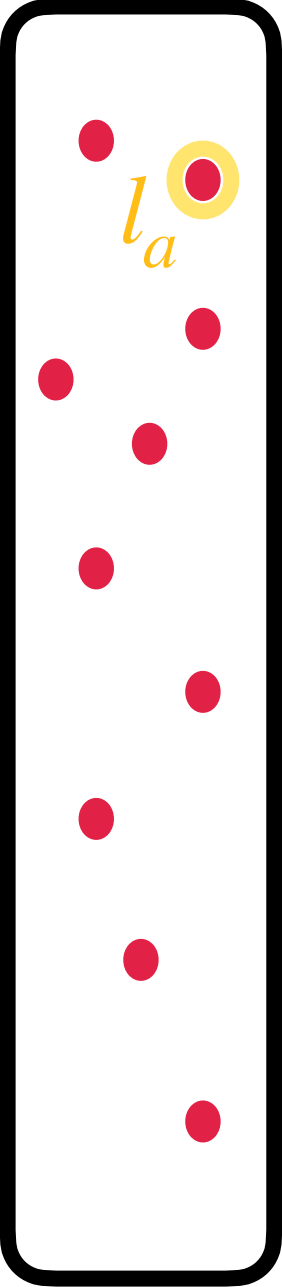
T_3 

Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

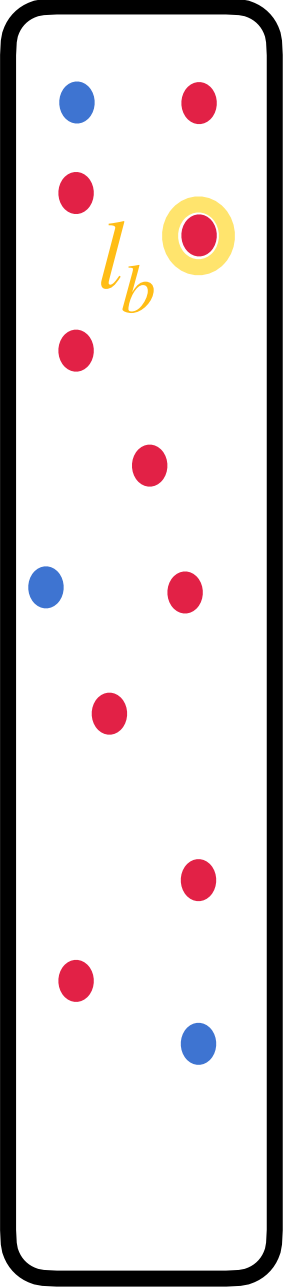
$C =$

T_1



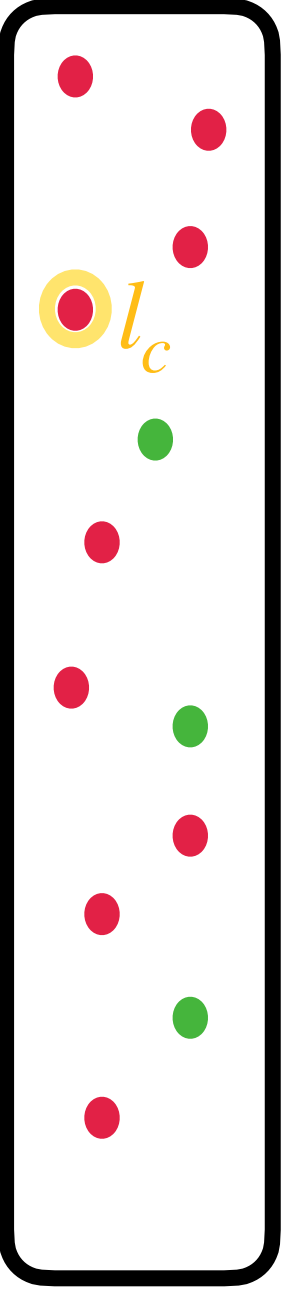
+

T_2



+

T_3



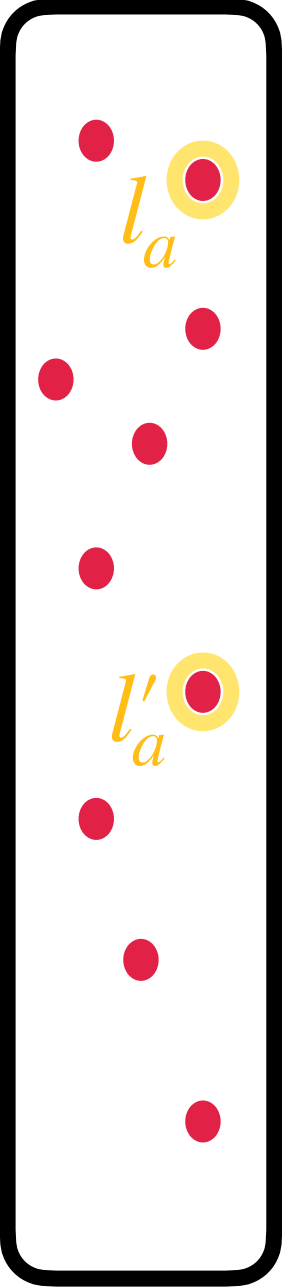
$\text{span}(l_1, l_2) \subset \text{span}(l_a, l_b, l_c)$

Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

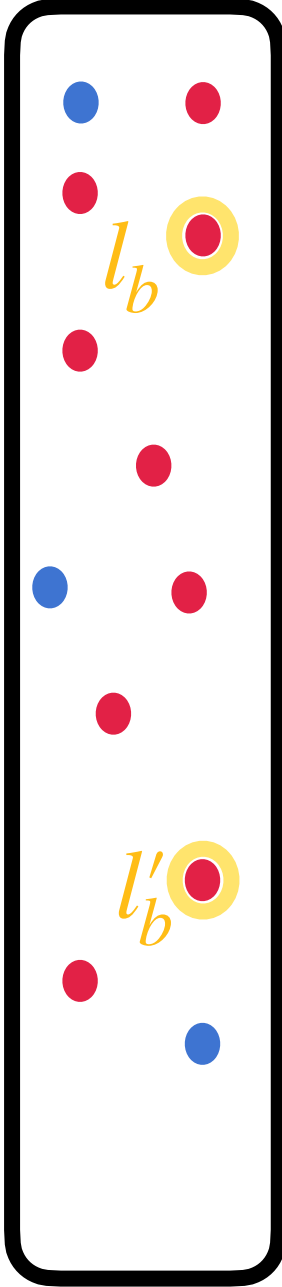
$C =$

T_1



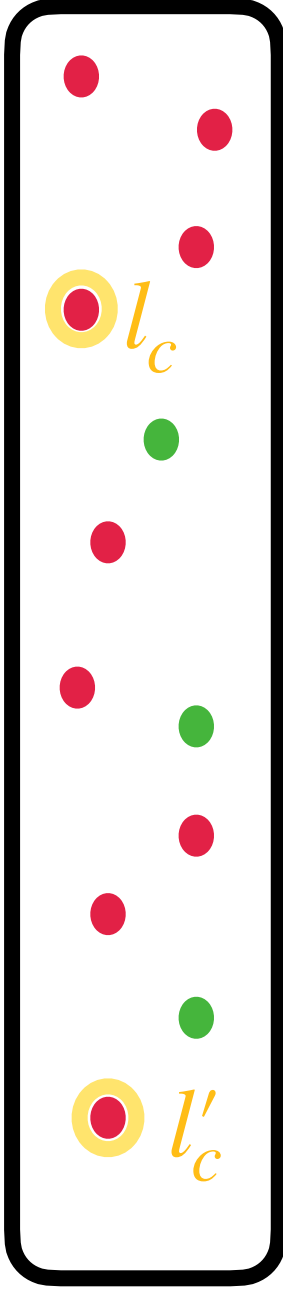
+

T_2



+

T_3



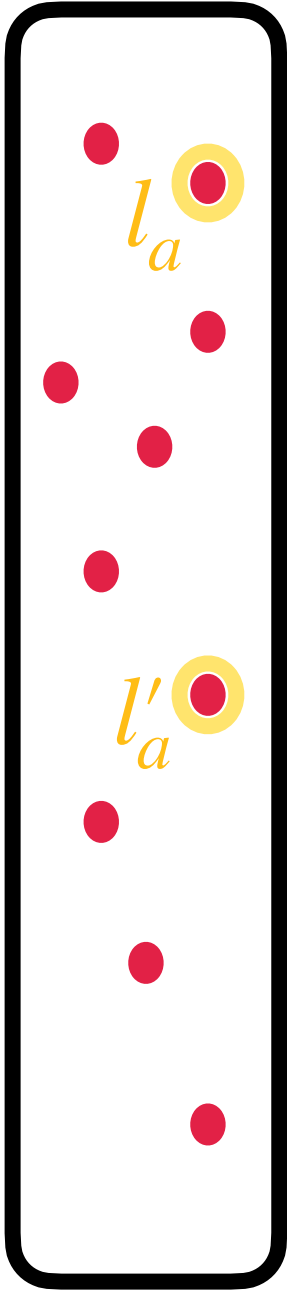
$\text{span}(l_1, l_2) \subset \text{span}(l_a, l_b, l_c)$

Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

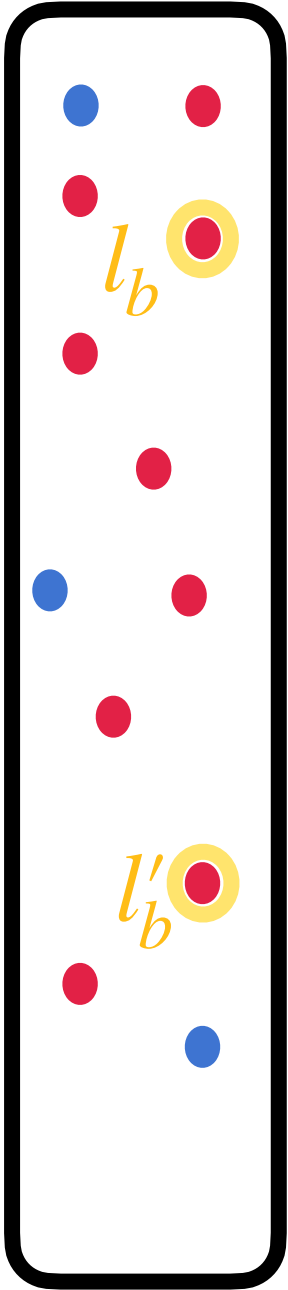
$C =$

T_1



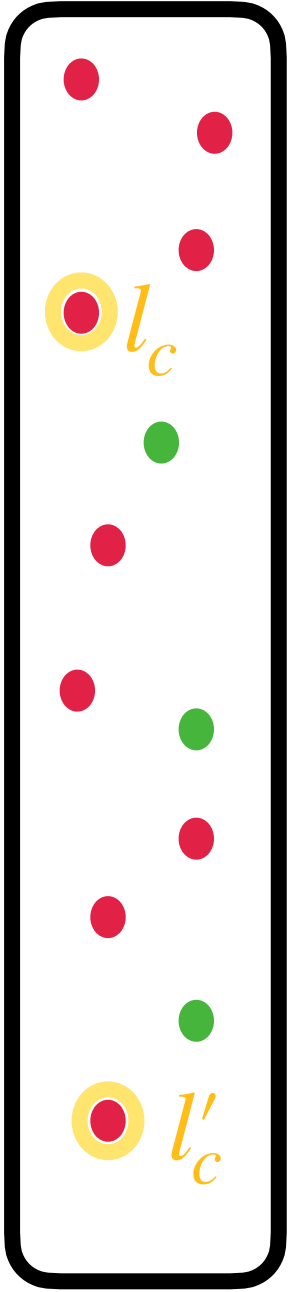
+

T_2



+

T_3

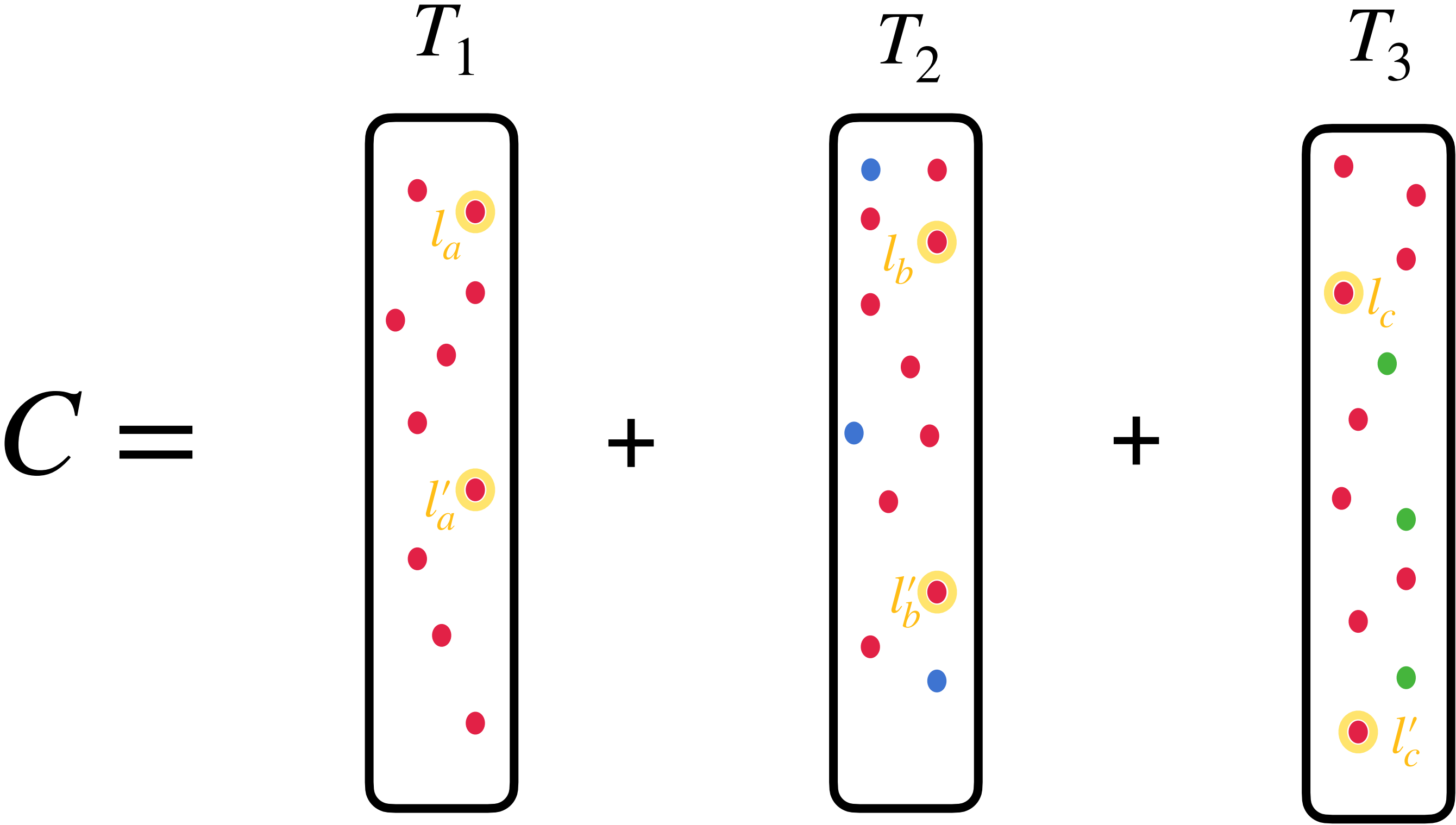


$\text{span}(l_1, l_2) \subset \text{span}(l_a, l_b, l_c)$

$\text{span}(l_1, l_2) \subset \text{span}(l'_a, l'_b, l'_c)$

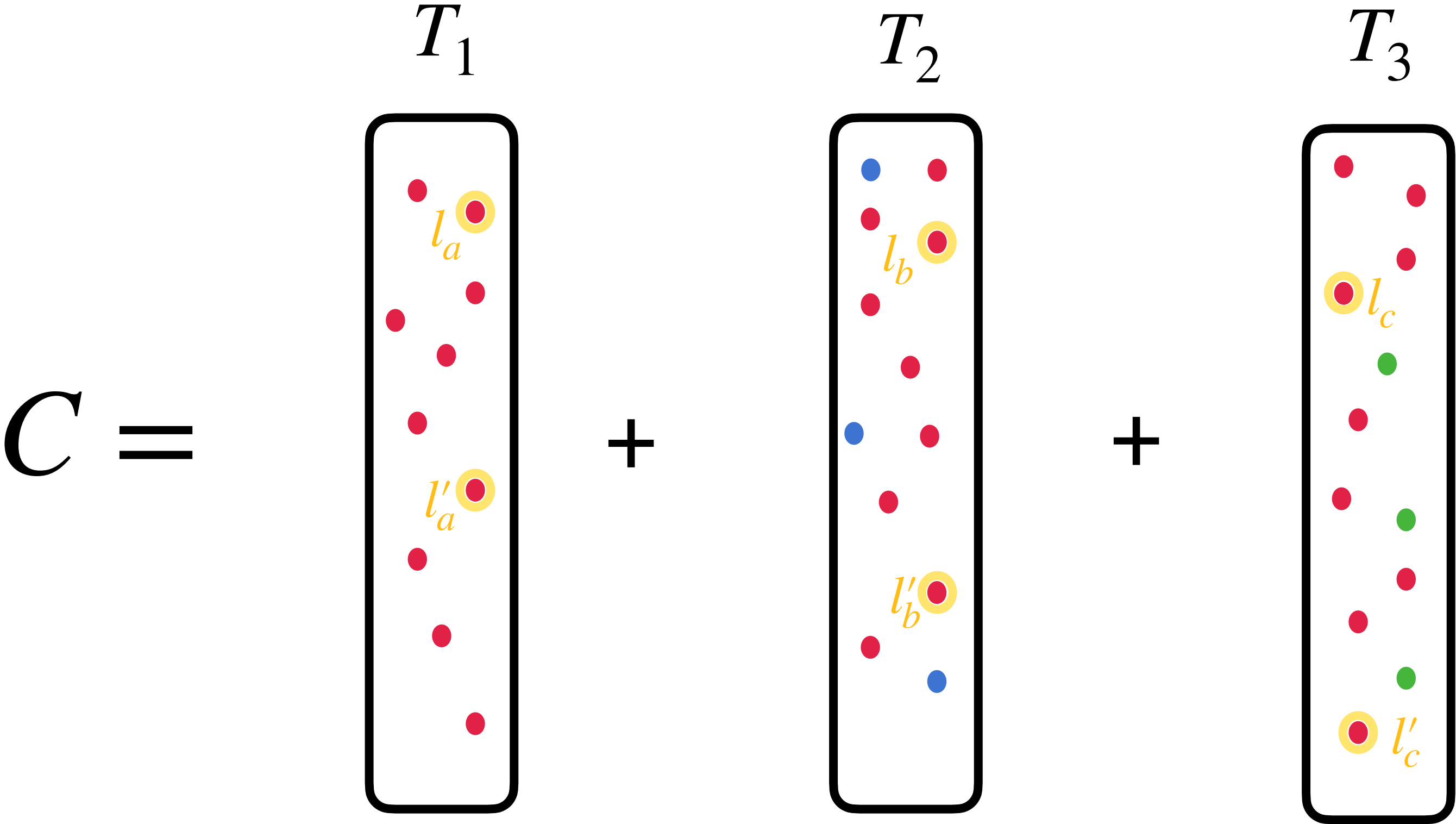
Bounding \mathcal{S}_2

$$\text{mod } \langle l_1, l_2 \rangle \quad \text{span}(l_1, l_2) = \text{span}(l_a, l_b, l_c) \cap \text{span}(l'_a, l'_b, l'_c)$$



Bounding \mathcal{S}_2

$$\text{mod } \langle l_1, l_2 \rangle \quad \text{span}(l_1, l_2) = \text{span}(l_a, l_b, l_c) \cap \text{span}(l'_a, l'_b, l'_c)$$

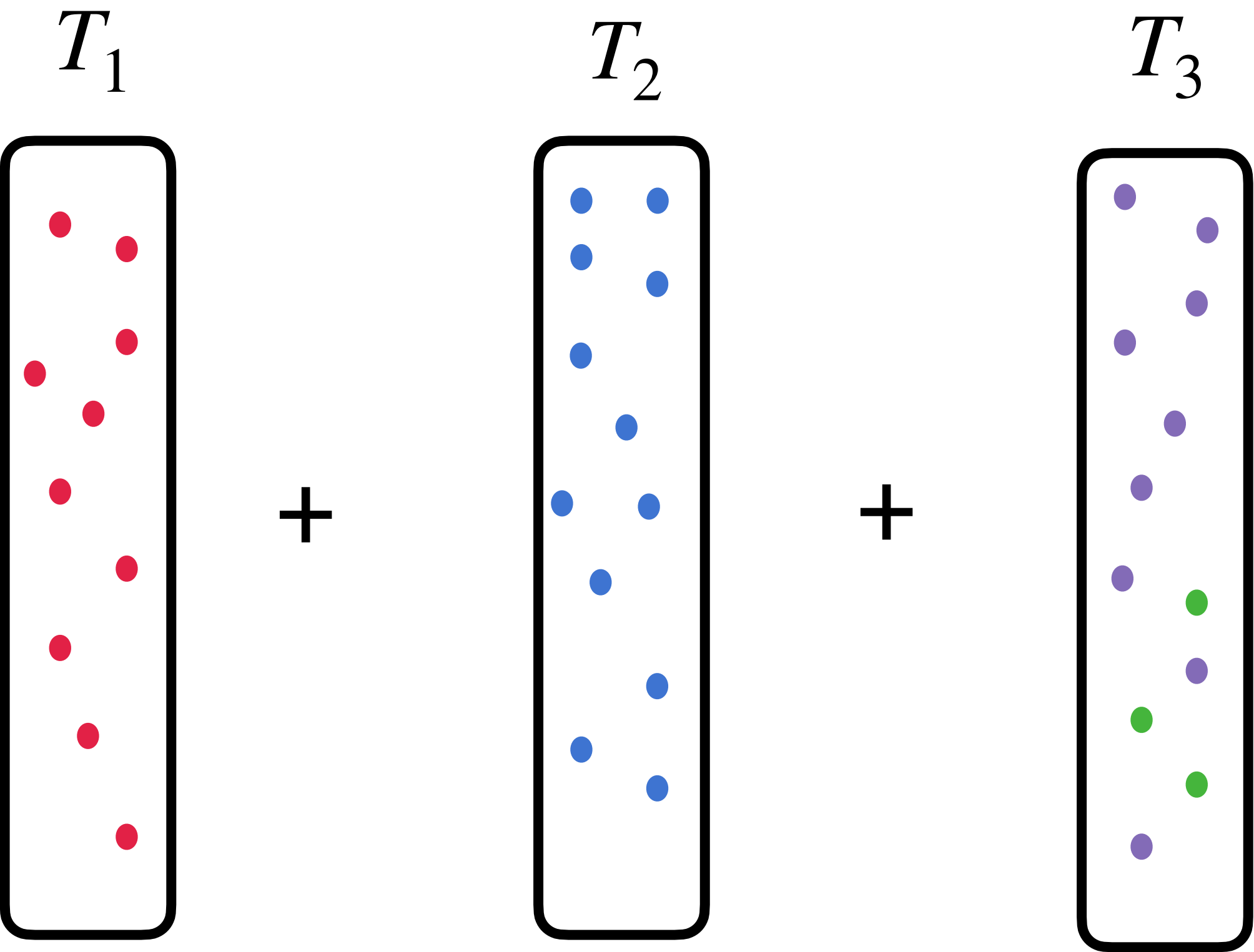


Number of possibilities for $\mathbb{V}(l_1, l_2)$ is at most d^6

Bounding \mathcal{S}_2

High Rank

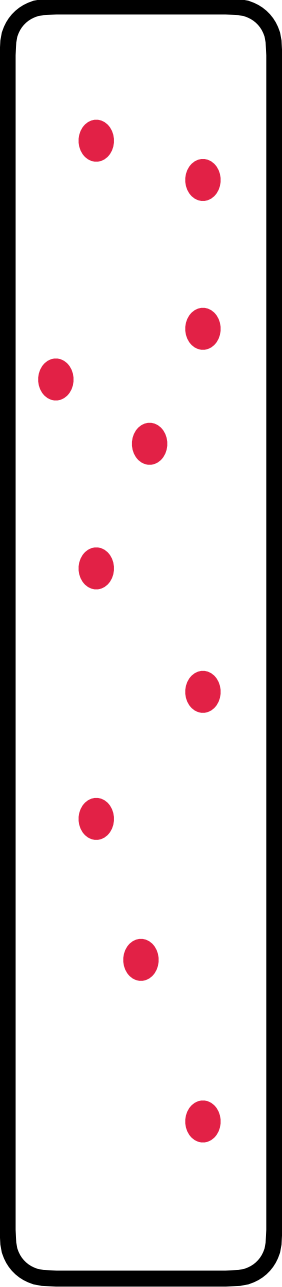
$C =$



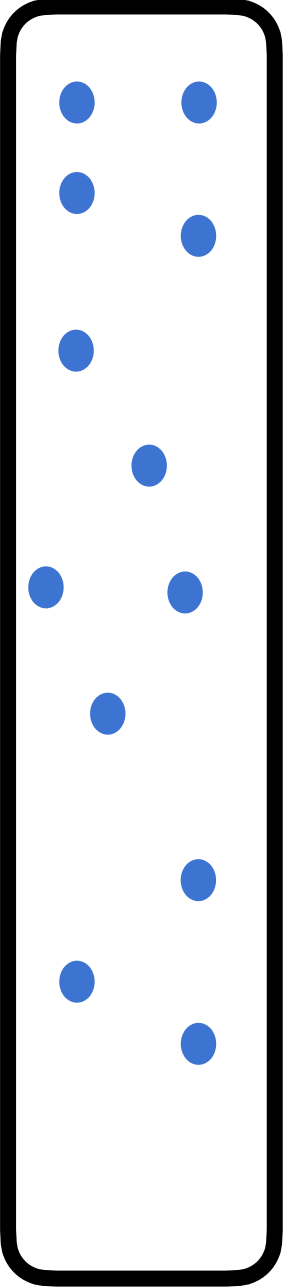
Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

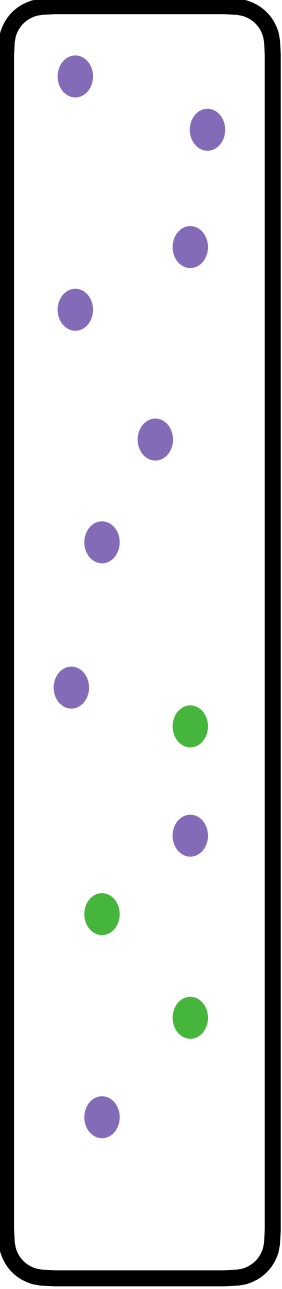
$C =$

T_1 

+

T_2 

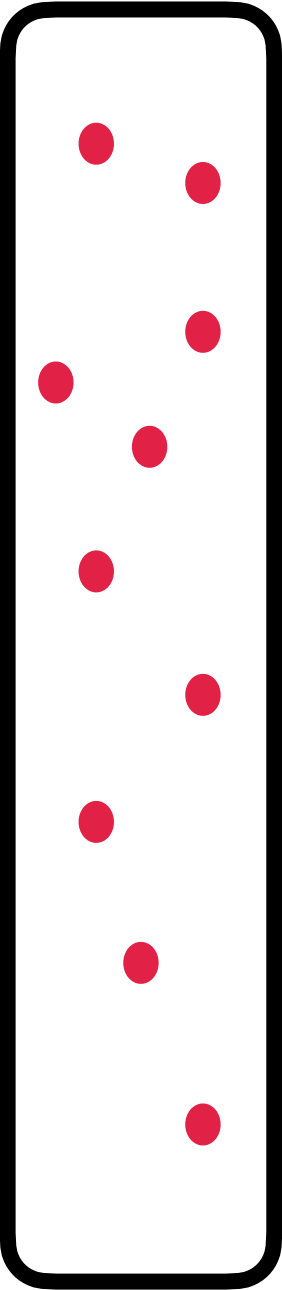
+

T_3 

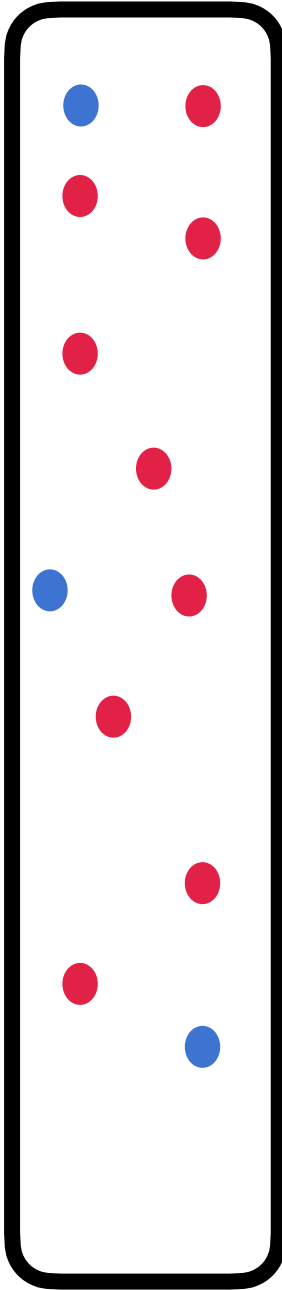
Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

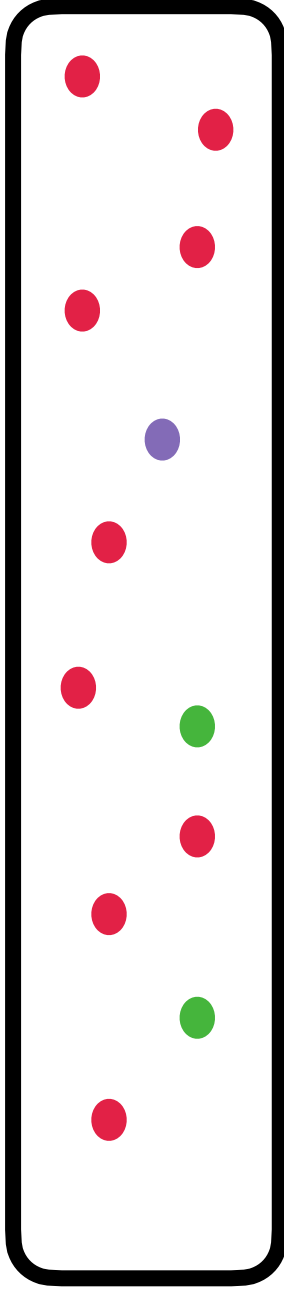
$C =$

T_1 

+

T_2 

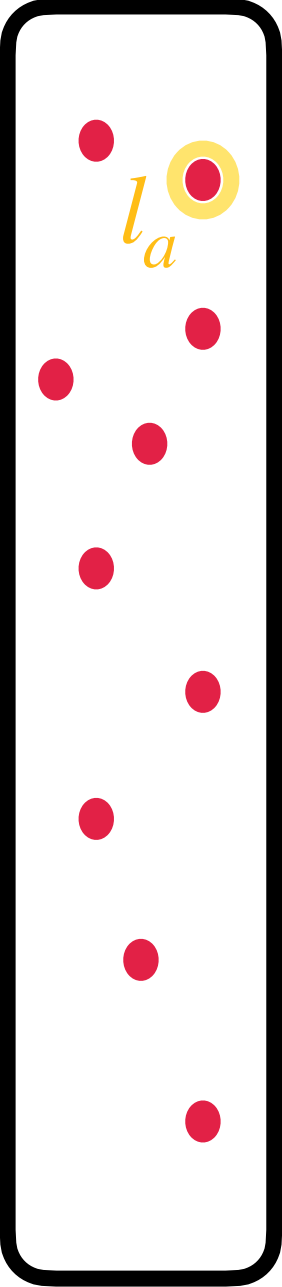
+

T_3 

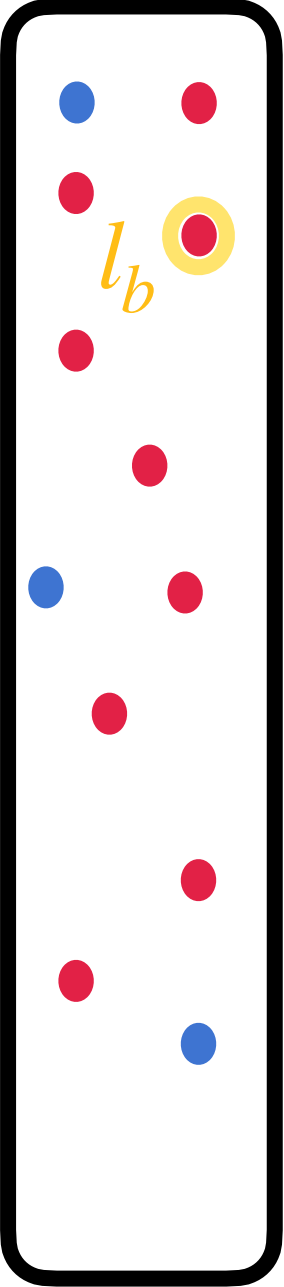
Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

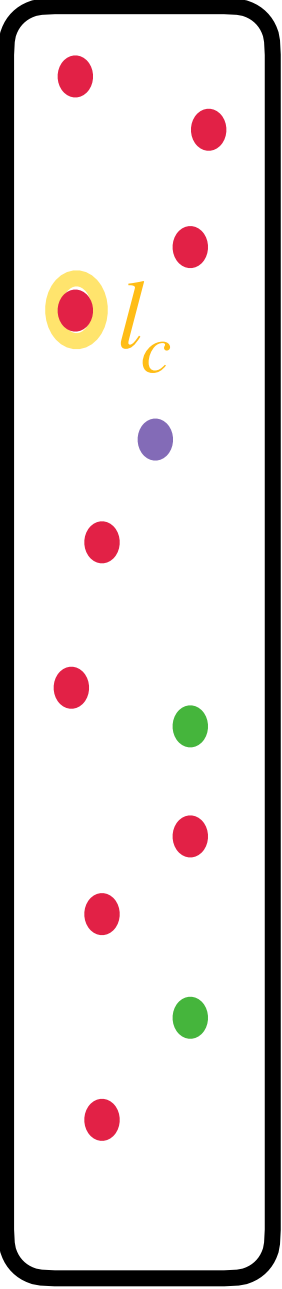
$C =$

T_1 

+

T_2 

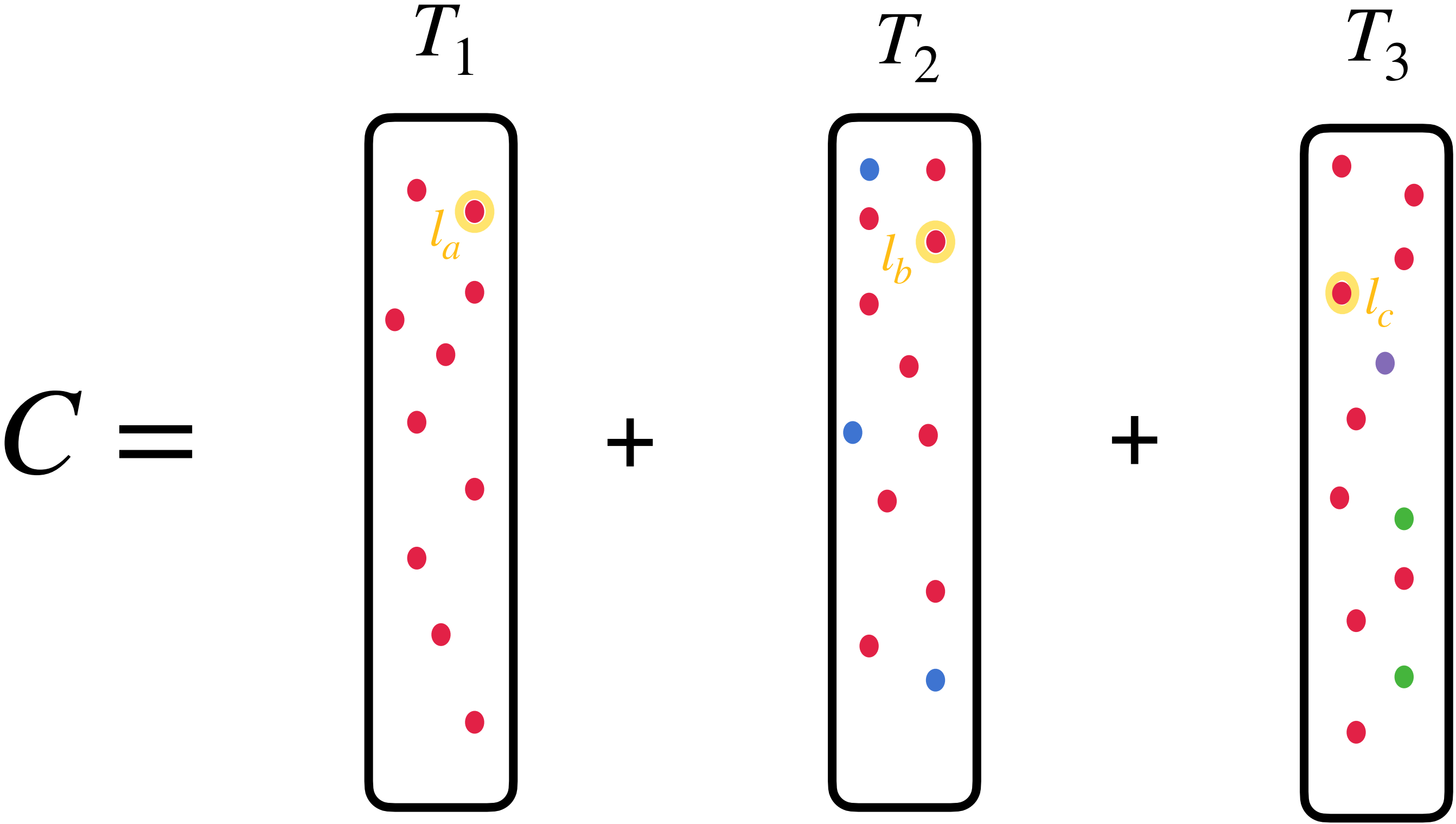
+

T_3 

Bounding \mathcal{S}_2

mod $\langle l_1, l_2 \rangle$

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$



Bounding \mathcal{S}_2

$\text{mod } \langle l_1, l_2 \rangle$

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

Diagram illustrating the decomposition of a set C into three subsets T_1 , T_2 , and T_3 .

The set C is represented by a large black-outlined rectangle. It is partitioned into three smaller rectangles labeled T_1 , T_2 , and T_3 .

Each subset T_i contains two yellow circles labeled l_i and l'_i .

- T_1 contains l_a and l'_a .
- T_2 contains l_b and l'_b .
- T_3 contains l_c and l'_c .

The circles are colored red, blue, or green. The diagram shows that C is the union of T_1 , T_2 , and T_3 .

Bounding \mathcal{S}_2

 $\text{mod } \langle l_1, l_2 \rangle$

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$

Diagram illustrating the decomposition of a set C into three subsets T_1 , T_2 , and T_3 .

The set C is represented by a large rectangle containing 10 red dots. The dots are grouped into three regions: the top region (labeled l_a), the middle region (labeled l'_a), and the bottom region (labeled l'_c).

The regions are separated by horizontal lines. The top region contains 4 dots, the middle region contains 4 dots, and the bottom region contains 2 dots.

The diagram shows that C is the union of T_1 , T_2 , and T_3 , where T_1 contains the top region, T_2 contains the middle region, and T_3 contains the bottom region.

Bounding \mathcal{S}_2

$$\text{mod } \langle l_1, l_2 \rangle$$

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$

Diagram illustrating the construction of C as the sum of three sets T_1 , T_2 , and T_3 .

T_1 contains points l_a and l'_a (yellow circles) and several red points.

T_2 contains points l_b and l'_b (yellow circles), blue points, and red points.

T_3 contains points l_c and l'_c (yellow circles), a purple point, green points, and red points.

The resulting set C is defined as:

$$C = T_1 + T_2 + T_3$$

Case 1: $l = l'$

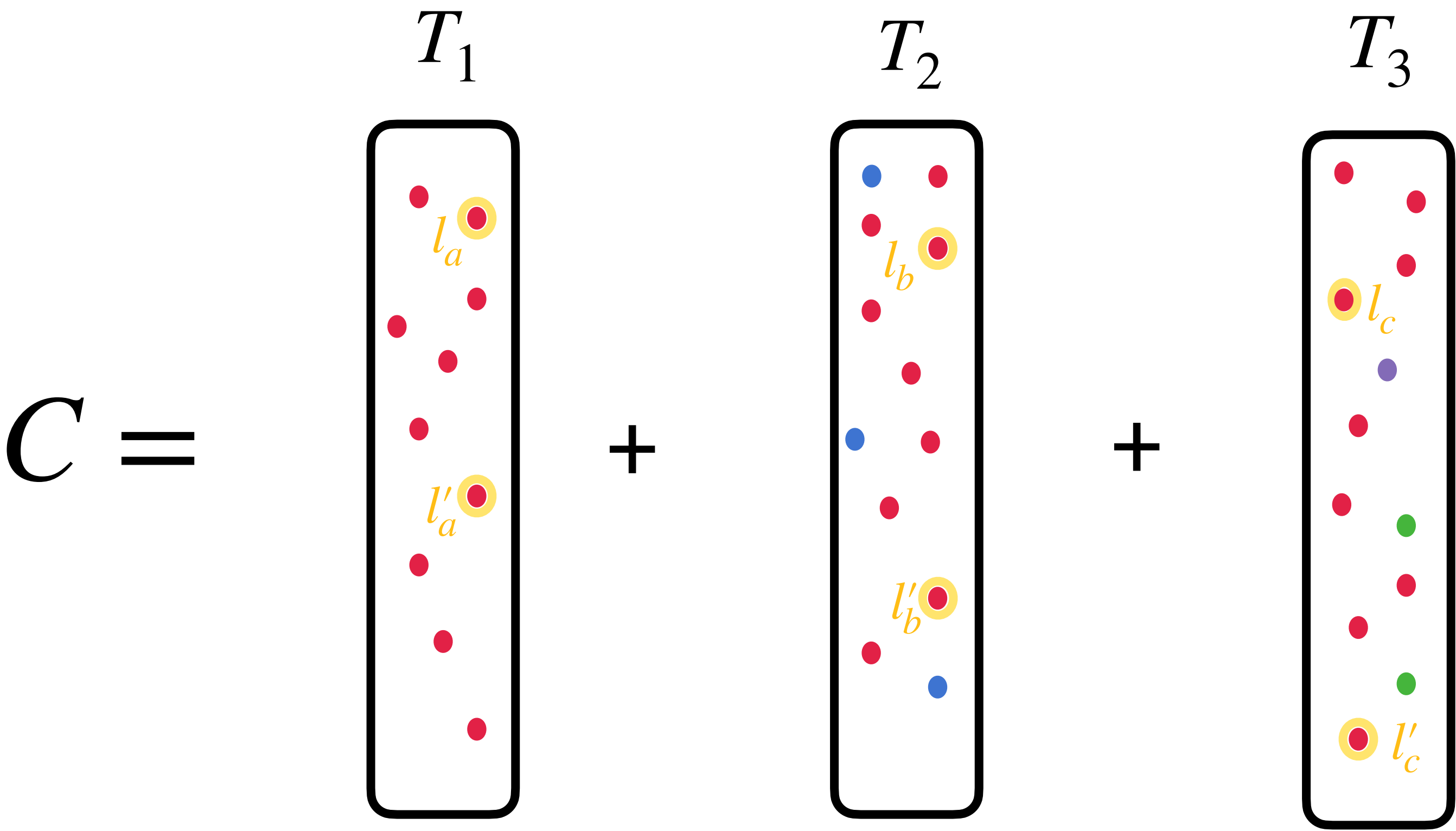
$\text{span}(l_a, l_b, l_c) \cap \text{span}(l'_a, l'_b, l'_c) \in \text{span}(l_1, l_2)$

Bounding \mathcal{S}_2

$$\text{mod } \langle l_1, l_2 \rangle$$

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$

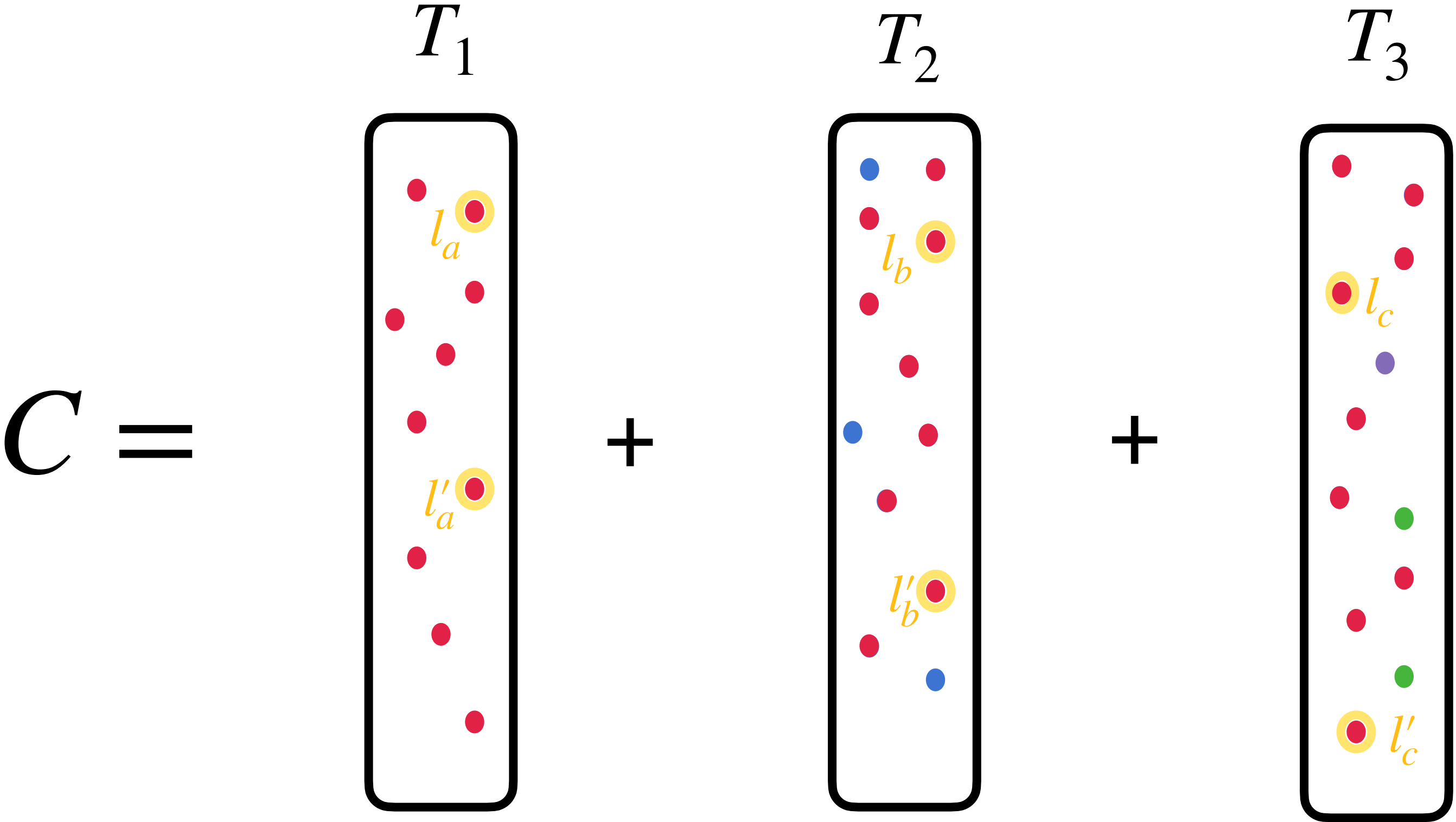


Bounding \mathcal{S}_2

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{mod } \langle l_1, l_2 \rangle$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$



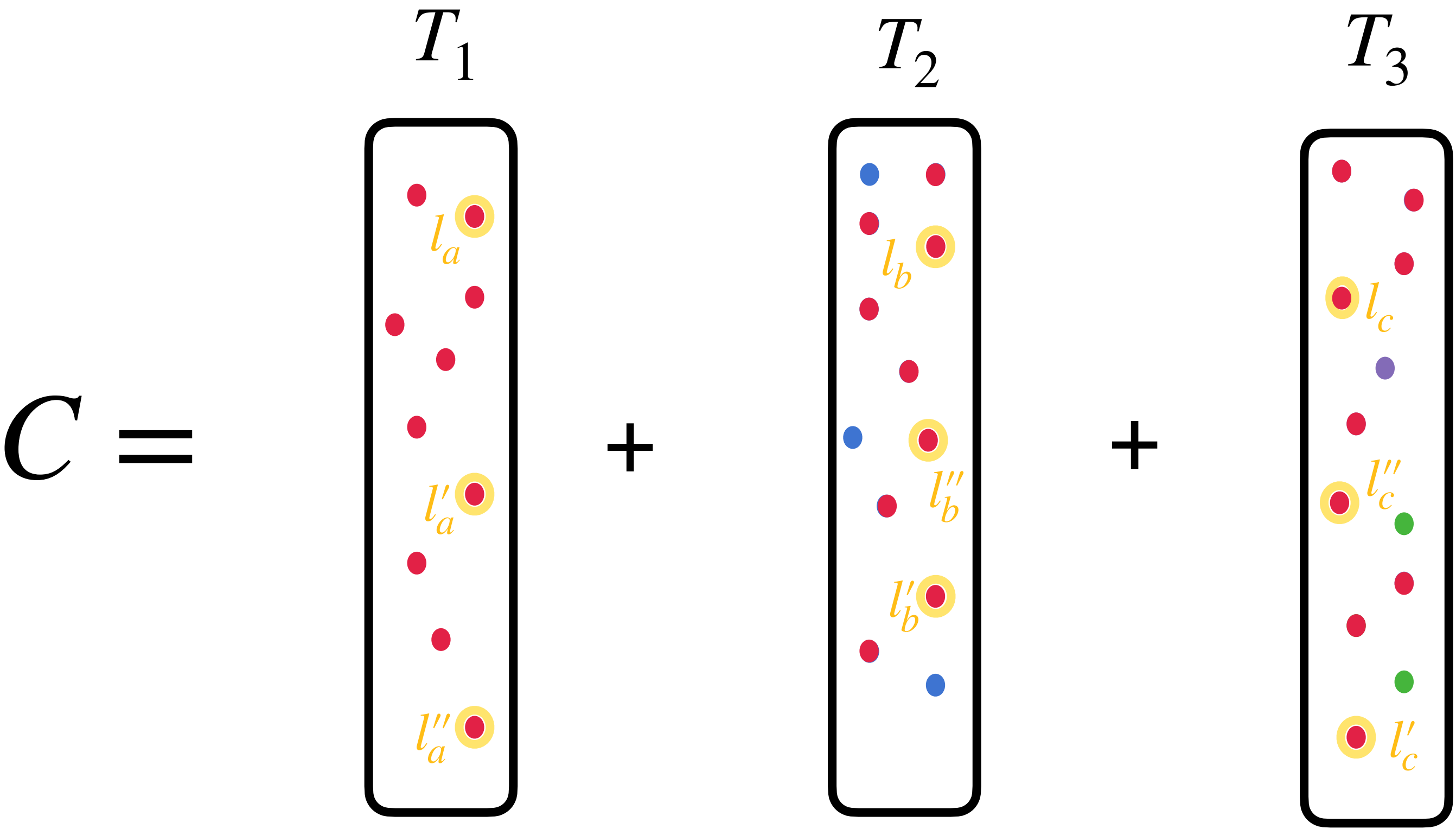
Bounding \mathcal{S}_2

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$

$$\text{span}(l_1, l_2) \cap \text{span}(l''_a, l''_b, l''_c) = \text{span}(l'')$$

mod $\langle l_1, l_2 \rangle$



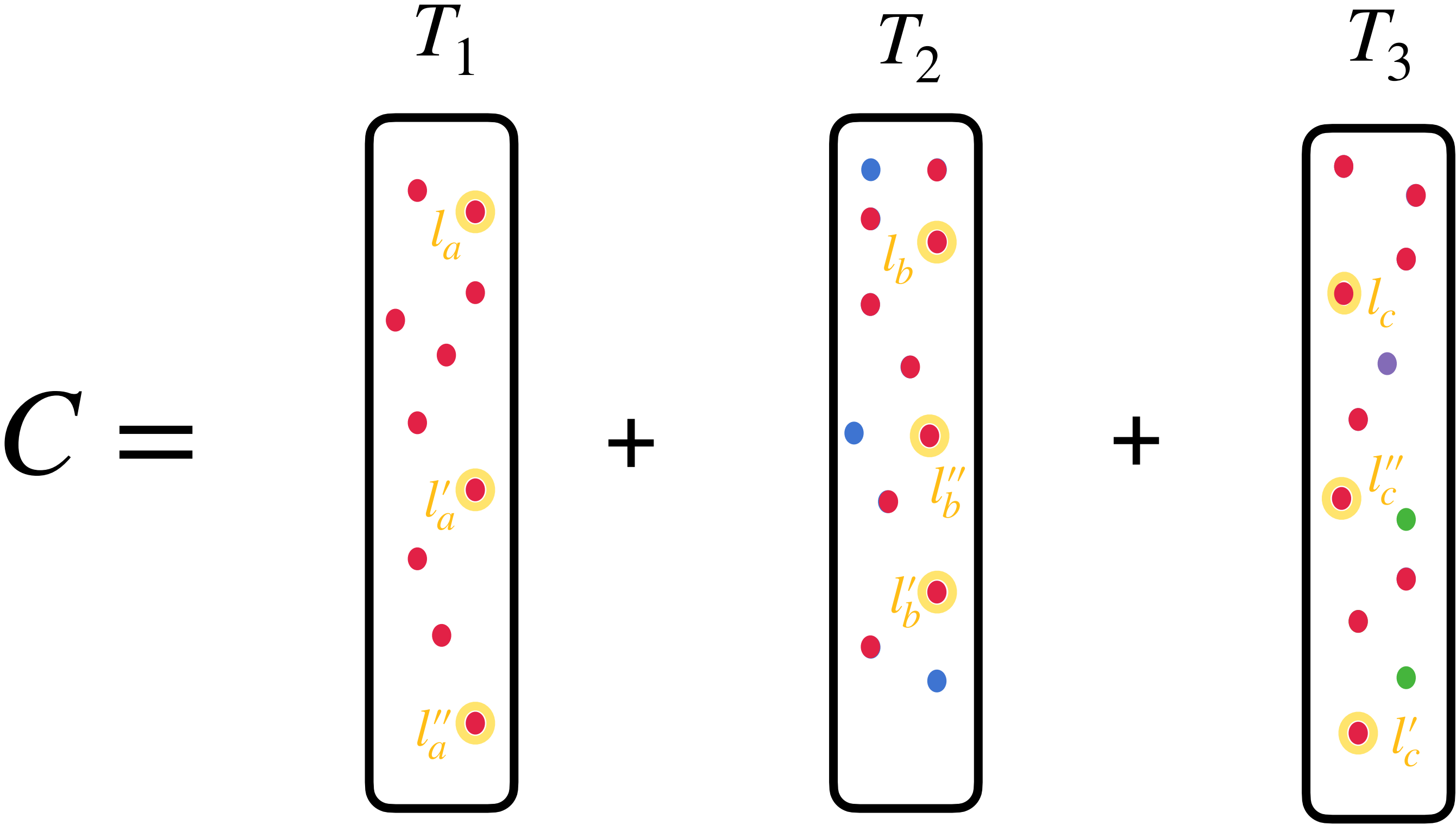
Bounding \mathcal{S}_2

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$

$$\text{span}(l_1, l_2) \cap \text{span}(l''_a, l''_b, l''_c) = \text{span}(l'')$$

mod $\langle l_1, l_2 \rangle$



Case 2: $l \neq l'$

$$\begin{aligned} &\text{span}(l_a, l_b, l_c, l'_a, l'_b, l'_c) \\ &\cap \\ &\text{span}(l''_a, l''_b, l''_c) \in \text{span}(l_1, l_2) \end{aligned}$$

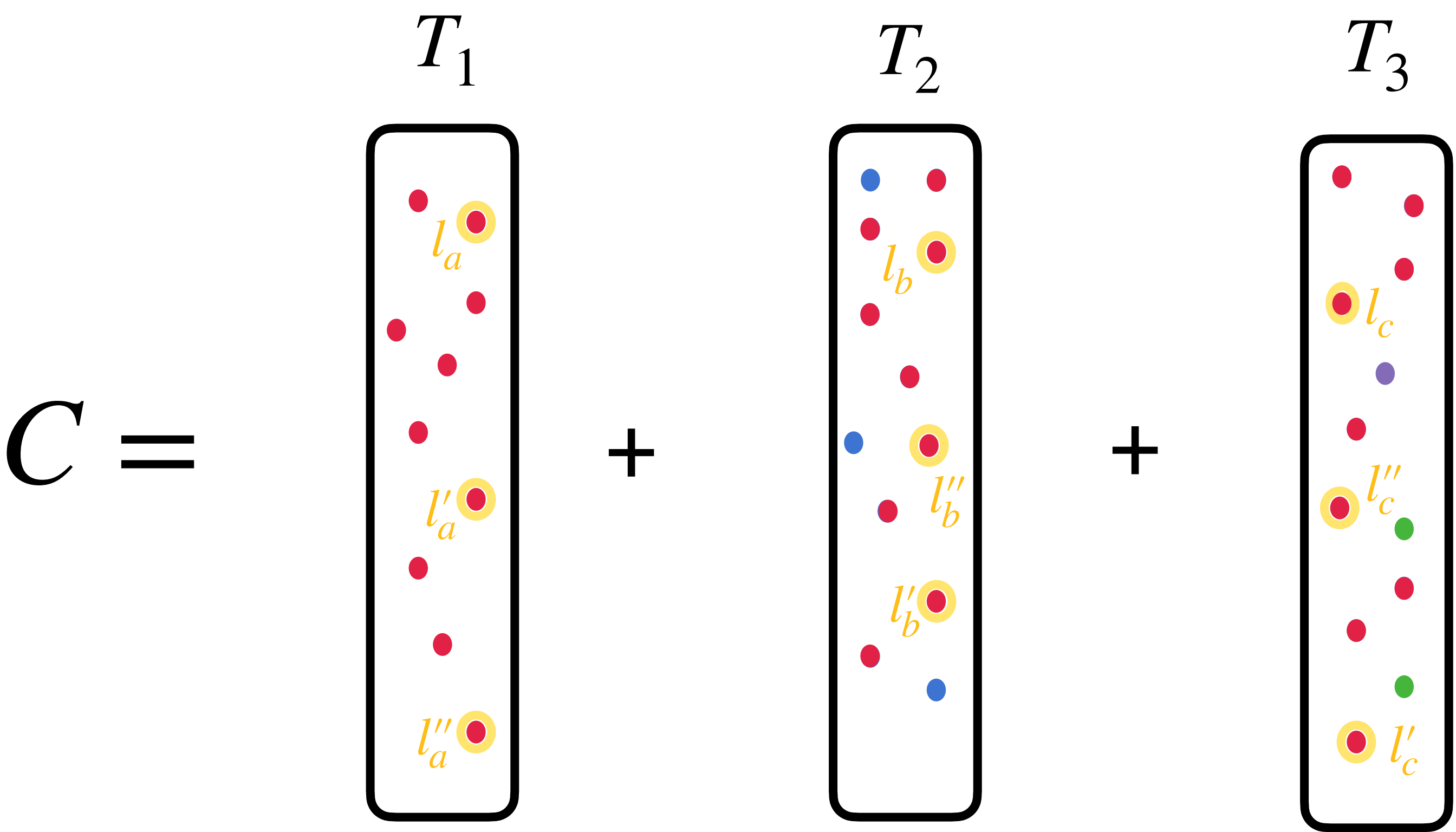
Bounding \mathcal{S}_2

$$\text{span}(l_1, l_2) \cap \text{span}(l_a, l_b, l_c) = \text{span}(l)$$

$$\text{span}(l_1, l_2) \cap \text{span}(l'_a, l'_b, l'_c) = \text{span}(l')$$

$$\text{span}(l_1, l_2) \cap \text{span}(l''_a, l''_b, l''_c) = \text{span}(l'')$$

mod $\langle l_1, l_2 \rangle$



Case 2: $l \neq l'$

$$\text{span}(l_a, l_b, l_c, l'_a, l'_b, l'_c)$$

$$\cap \text{span}(l''_a, l''_b, l''_c) \in \text{span}(l_1, l_2)$$

Number of possibilities for

$\mathbb{V}(l_1, l_2)$ is at most d^7

Future Work

- Reconstruction for $\Sigma\Pi\Sigma(k)$ circuits for $k > 3$.
- Proper Learning when rank is *small*.

Thank You

Questions?