The Quantitative Combinatorial Nullstellensatz and Integer-Valued Polynomials

Uwe Schauz

uwe.schauz@xjtlu.edu.cn

Xi'an Jiaotong-Liverpool University, Suzhou, China

Lille, June 24, 2013

Theorem (Quantitative Combinatorial Nullstellensatz)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$, $d_j := |I_j| - 1$, *and let* $P \in \mathbb{F}[X_1, X_2, \ldots, X_n]$.
If $\deg(P) \leq |I_1| + |I_2| + \cdots + |I_n| - n = d_1 + d_2 + \cdots + d_n$ *then for the coefficient* $P_{d_1,d_2,\ldots,d_n}$ *of the monomial* $X_1^{d_1} X_2^{d_2} \cdots X_n^{d_n}$ *in* P *the following holds:*

$$P_{d_1,d_2,\ldots,d_n} = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x) P(x) \ ,$$

with a certain map $M \colon I_1 \times I_2 \times \cdots \times I_n \longrightarrow \mathbb{F}$ *not depending on* P.

Theorem (Quantitative Combinatorial Nullstellensatz)

Let $I := I_1 \times \cdots \times I_n \subseteq \mathbb{F}^n$ *and set* $d_j := |I_j| - 1$, $d := (d_j)$.

For polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}[X_1, \ldots, X_n]$ *of total degree* $\deg(P) \leq \Sigma_j \, d_j$,

$$P_d = \sum_{x \in I} N(x)^{-1} P(x) \ ,$$

where $N(x_1, \ldots, x_n) := \prod_j \prod_{\xi \in I_j \setminus x_j} (x_j - \xi) \neq 0$.

Corollaries

(i) $P_d \neq 0 \implies \left| \{ \, x \in I \mid P(x) \neq 0 \, \} \right| \neq 0$.

(ii) $\deg(P) < \Sigma_j \, d_j \implies P_d = 0 \implies \left| \{ \, x \in I \mid P(x) \neq 0 \, \} \right| \neq 1$.

(iii) If $\mathbb{F} := \mathbb{F}_q$ and $P_1, \ldots, P_m \in \mathbb{F}[X_1, \ldots, X_n]$ then

$$\sum_i \deg(P_i) < \frac{\Sigma_j \, d_j}{q-1} \implies \left| \{ \, x \in I \mid P_1(x) = \cdots = P_m(x) = 0 \, \} \right| \neq 1 \ .$$

Theorem (Quantitative Combinatorial Nullstellensatz)

Let $I := I_1 \times \cdots \times I_n \subseteq \mathbb{F}^n$ *and set* $d_j := |I_j| - 1$, $d := (d_j)$.

For polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}[X_1, \ldots, X_n]$ *of total degree* $\deg(P) \leq \Sigma_j \, d_j$,

$$P_d = \sum_{x \in I} N(x)^{-1} P(x) \ ,$$

where $N(x_1, \ldots, x_n) := \prod_j \prod_{\xi \in I_j \setminus x_j} (x_j - \xi) \neq 0$.

Corollaries

(i) $$P_d \neq 0 \implies \big|\{ x \in I \mid P(x) \neq 0 \}\big| \neq 0 \ .$$

(ii) $$\deg(P) < \Sigma_j \, d_j \implies P_d = 0 \implies \big|\{ x \in I \mid P(x) \neq 0 \}\big| \neq 1 \ .$$

(iii) If $\mathbb{F} := \mathbb{F}_q$ and $P_1, \ldots, P_m \in \mathbb{F}[X_1, \ldots, X_n]$ then

$$\sum_i \deg(P_i) < \frac{\Sigma_j \, d_j}{q-1} \implies \big|\{ x \in I \mid P_1(x) = \cdots = P_m(x) = 0 \}\big| \neq 1 \ .$$

Theorem (Interpolation Formula)

Let $I \subseteq \mathbb{F}^n$ be a d-grid over a field $\mathbb{F}$ and $y : I \longrightarrow \mathbb{F}$ a map.

There exists a unique polynomial $P \in \mathbb{F}[X_1, \ldots, X_n]$ with partial degrees $\deg_j(P) \leq d_j$ that interpolates y, i.e., $P|_I = y$.

The coefficients P_δ of P are given by

$$P_\delta = \sum_{x \in I} M_\delta(x)\, y(x) \ ,$$

with certain maps $M_\delta : I \longrightarrow \mathbb{F}$.

Corollary (Inversion Formula)

Polynomials $P \in \mathbb{F}[X_1, \ldots, X_n]$ with partial degrees $\deg_j(P) \leq d_j$ are uniquely determined by $P|_I$. The coefficients P_δ of P are given by

$$P_\delta = \sum_{x \in I} M_\delta(x)\, P(x) \ .$$

Theorem (Interpolation Formula)

Let $I \subseteq \mathbb{F}^n$ *be a d-grid over a field* $\mathbb{F}$ *and* $y\colon I \longrightarrow \mathbb{F}$ *a map.*

There exists a unique polynomial $P \in \mathbb{F}[X_1, \ldots, X_n]$ *with partial degrees* $\deg_j(P) \leq d_j$ *that interpolates* y *, i.e.,* $P|_I = y$ *.*

The coefficients P_δ *of* P *are given by*

$$P_\delta = \sum_{x \in I} M_\delta(x)\, y(x) \ ,$$

with certain maps $M_\delta\colon I \longrightarrow \mathbb{F}$ *.*

Corollary (Inversion Formula)

Polynomials $P \in \mathbb{F}[X_1, \ldots, X_n]$ *with partial degrees* $\deg_j(P) \leq d_j$ *are uniquely determined by* $P|_I$ *. The coefficients* P_δ *of* P *are given by*

$$P_\delta = \sum_{x \in I} M_\delta(x)\, P(x) \ .$$

Theorem (Interpolation Formula)

Let $I \subseteq \mathbb{F}^n$ *be a d-grid over a field* $\mathbb{F}$ *and* $y\colon I \longrightarrow \mathbb{F}$ *a map.*

There exists a unique polynomial $P \in \mathbb{F}[X_1, \ldots, X_n]$ *with partial degrees* $\deg_j(P) \leq d_j$ *that interpolates* y *, i.e.,* $P|_I = y$ *.*

The coefficients P_δ *of* P *are given by*

$$P_\delta = \sum_{x \in I} M_\delta(x)\, y(x) \ ,$$

with certain maps $M_\delta\colon I \longrightarrow \mathbb{F}$ *.*

Corollary (Inversion Formula)

Polynomials $P \in \mathbb{F}[X_1, \ldots, X_n]$ *with partial degrees* $\deg_j(P) \leq d_j$ *are uniquely determined by* $P|_I$ *. The coefficients* P_δ *of* P *are given by*

$$P_\delta = \sum_{x \in I} M_\delta(x)\, P(x) \ .$$

Theorem (Interpolation Formula)

Let $I \subseteq \mathbb{F}^n$ *be a d-grid over a field* $\mathbb{F}$ *and* $y\colon I \longrightarrow \mathbb{F}$ *a map.*

There exists a unique polynomial $P \in \mathbb{F}[X_1, \ldots, X_n]$ *with partial degrees* $\deg_j(P) \leq d_j$ *that interpolates* y *, i.e.,* $P|_I = y$ *.*

The coefficients P_δ *of* P *are given by*

$$P_\delta = \sum_{x \in I} M_\delta(x)\, y(x) \ ,$$

with certain maps $M_\delta\colon I \longrightarrow \mathbb{F}$ *.*

Corollary (Inversion Formula)

Polynomials $P \in \mathbb{F}[X_1, \ldots, X_n]$ *with partial degrees* $\deg_j(P) \leq d_j$ *are uniquely determined by* $P|_I$ *. The coefficients* P_δ *of* P *are given by*

$$P_\delta = \sum_{x \in I} M_\delta(x)\, P(x) \ .$$

Proof of the Quantitative Combinatorial Nullstellensatz.

Transform P into a *trimmed* polynomial P/I with

(i) $(P/I)(x) = P(x)$ for all $x \in I$,

(ii) $(P/I)_d = P_d$,

(iii) $\deg_j(P/I) \leq d_j$ for $j = 1, \ldots, n$.

Then

$$P_d \overset{(ii)}{=} (P/I)_d \overset{(iii)}{=} \sum_{x \in I} M_d(x)\,(P/I)(x) \overset{(i)}{=} \sum_{x \in I} M_d(x)\,P(x)\,.$$

□

Proof of the Quantitative Combinatorial Nullstellensatz.

Transform P into a *trimmed* polynomial P/I with

(i) $(P/I)(x) = P(x)$ for all $x \in I$,

(ii) $(P/I)_d = P_d$,

(iii) $\deg_j(P/I) \leq d_j$ for $j = 1, \ldots, n$.

Then

$$P_d \overset{(ii)}{=} (P/I)_d \overset{(iii)}{=} \sum_{x \in I} M_d(x)\,(P/I)(x) \overset{(i)}{=} \sum_{x \in I} M_d(x)\,P(x)\,.$$

□

Proof of the Quantitative Combinatorial Nullstellensatz.

Transform P into a *trimmed* polynomial P/I with

(i) $(P/I)(x) = P(x)$ for all $x \in I$,

(ii) $(P/I)_d = P_d$,

(iii) $\deg_j(P/I) \leq d_j$ for $j = 1, \ldots, n$.

Then

$$P_d \overset{(ii)}{=} (P/I)_d \overset{(iii)}{=} \sum_{x \in I} M_d(x)\,(P/I)(x) \overset{(i)}{=} \sum_{x \in I} M_d(x)\,P(x)\,.$$

□

Proof of the Quantitative Combinatorial Nullstellensatz.

Transform P into a *trimmed* polynomial P/I with

(i) $(P/I)(x) = P(x)$ for all $x \in I$,

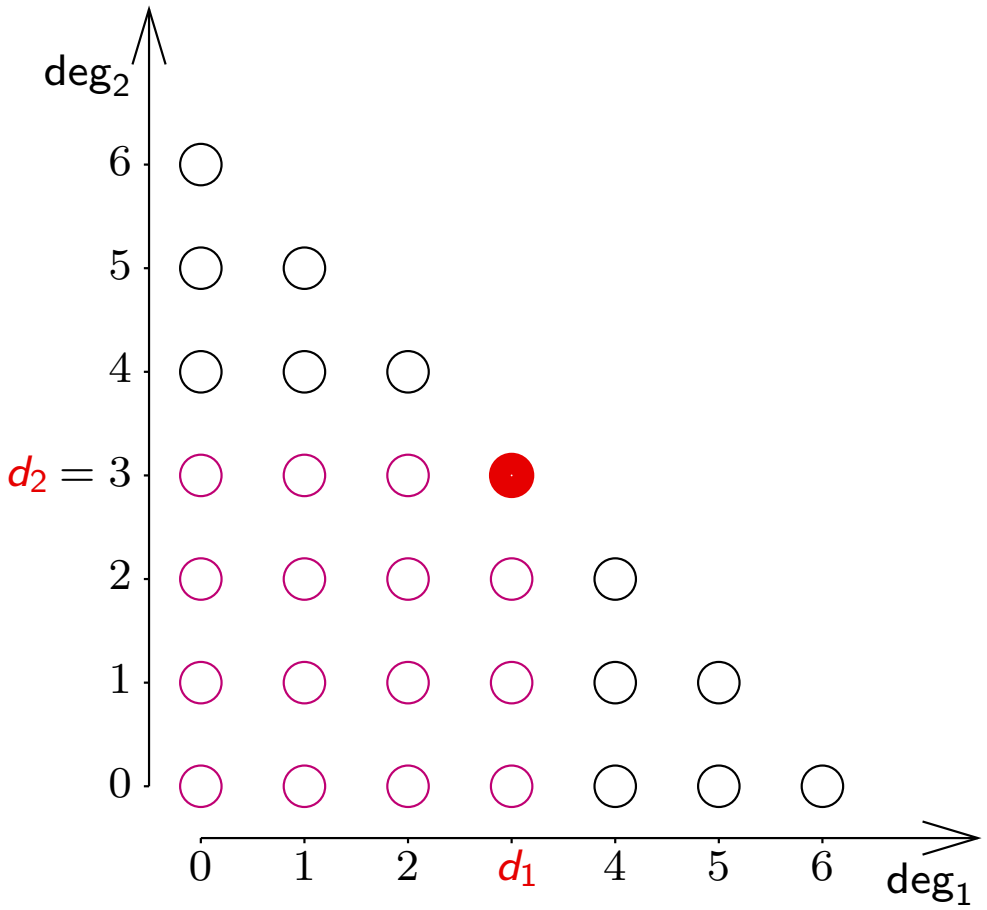
(ii) $(P/I)_d = P_d$,

(iii) $\deg_j(P/I) \leq d_j$ for $j = 1, \ldots, n$.

Then

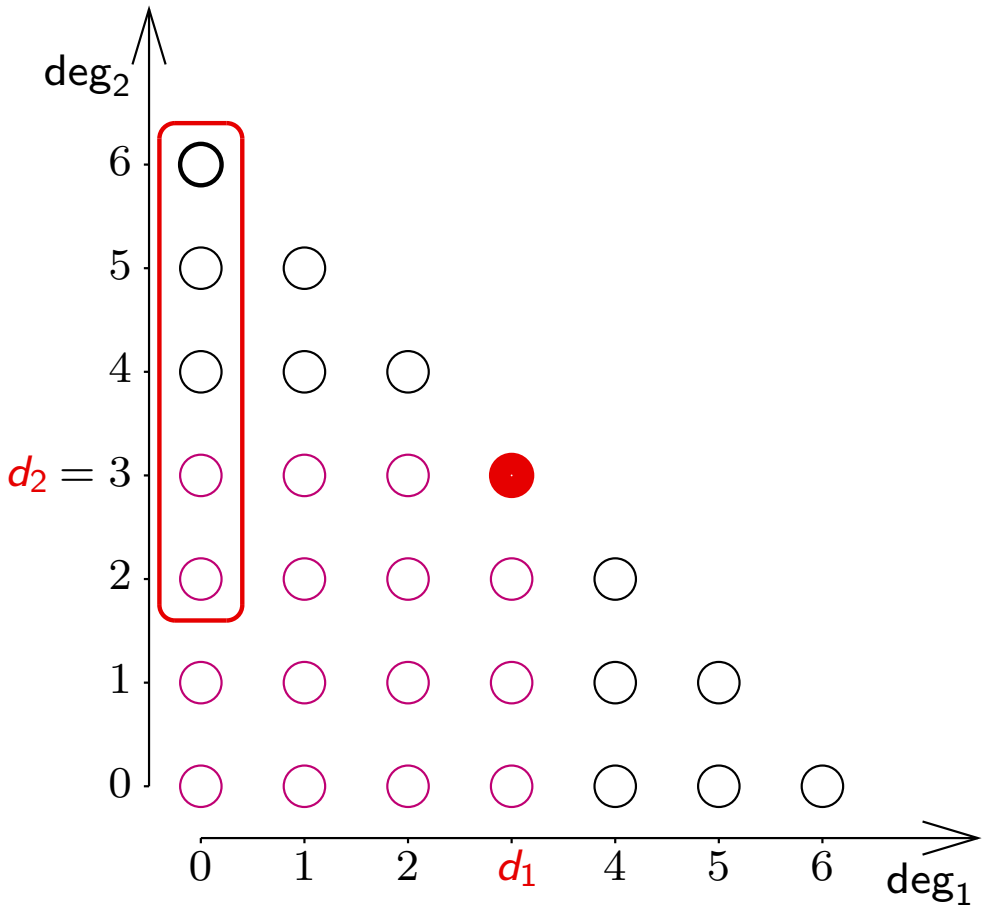
$$P_d \overset{(ii)}{=} (P/I)_d \overset{(iii)}{=} \sum_{x \in I} M_d(x)\,(P/I)(x) \overset{(i)}{=} \sum_{x \in I} M_d(x)\,P(x)\ .$$

The transformation $P \longmapsto\longmapsto \cdots \longmapsto P/\mathfrak{X}$:



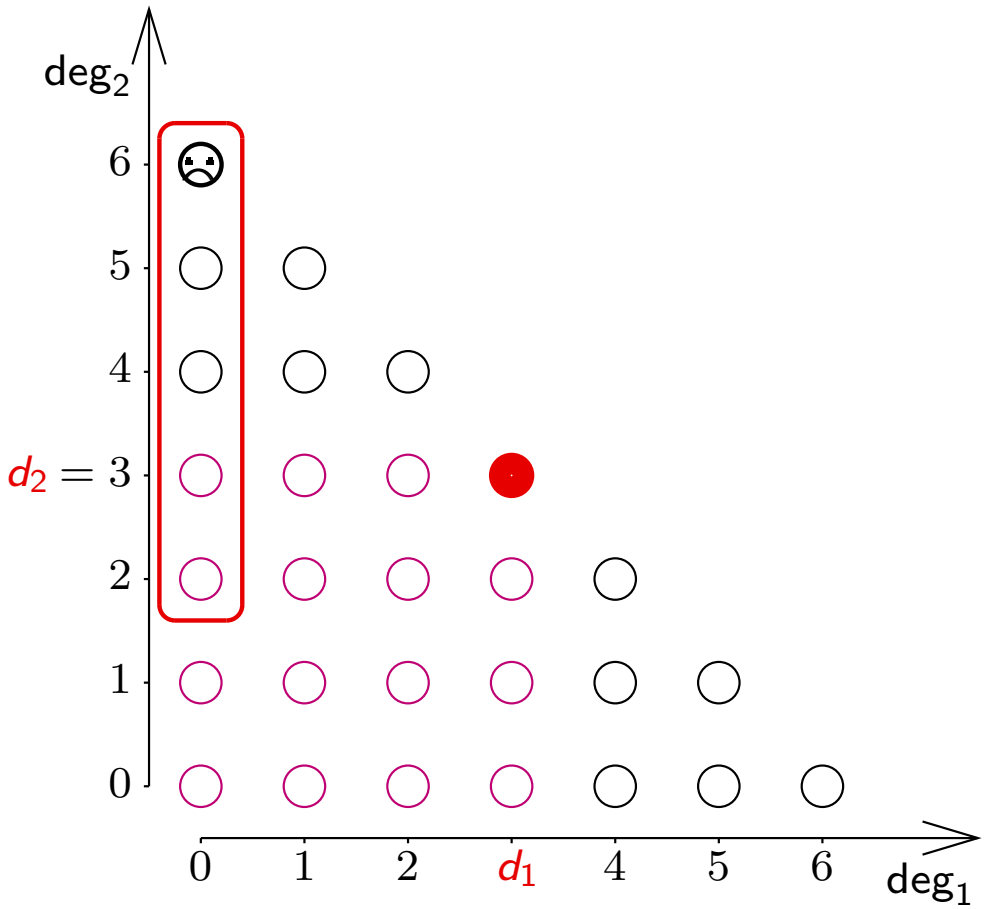
Start with P and add successively ...

The transformation $P \longmapsto\longmapsto \cdots \longmapsto P/\mathfrak{X}$:



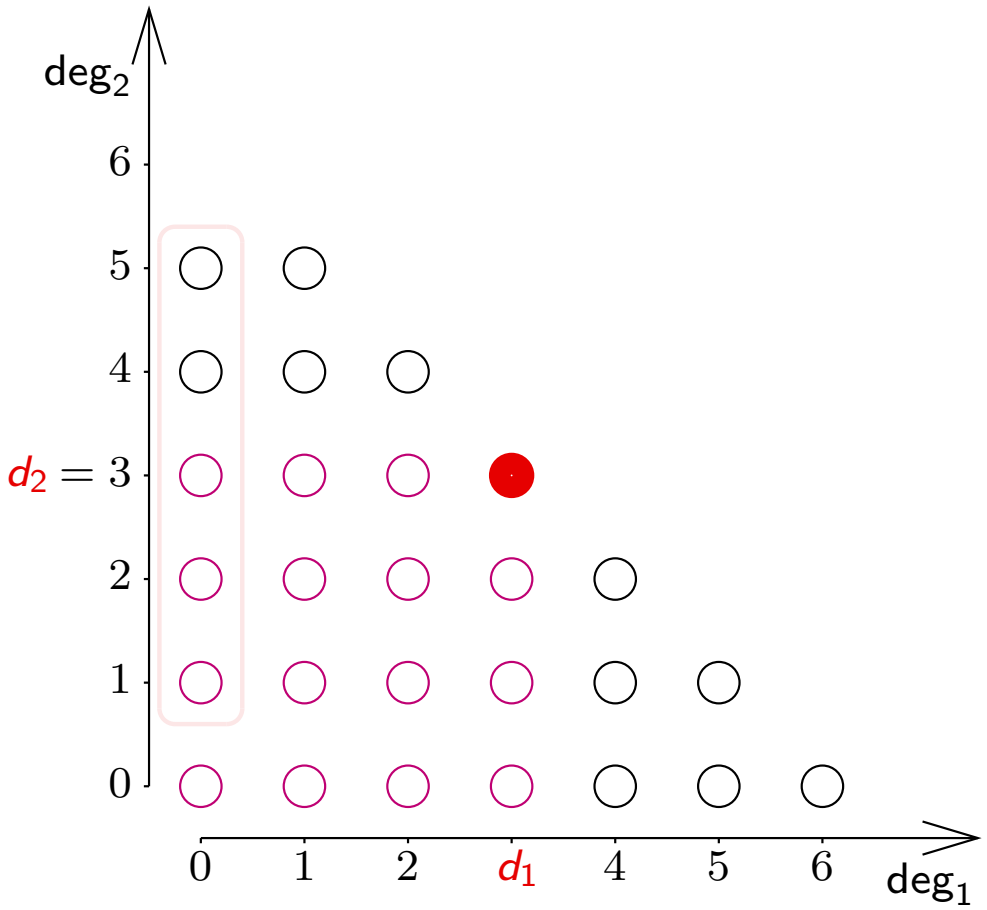
$$+ \quad c \; X^{(0,2)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



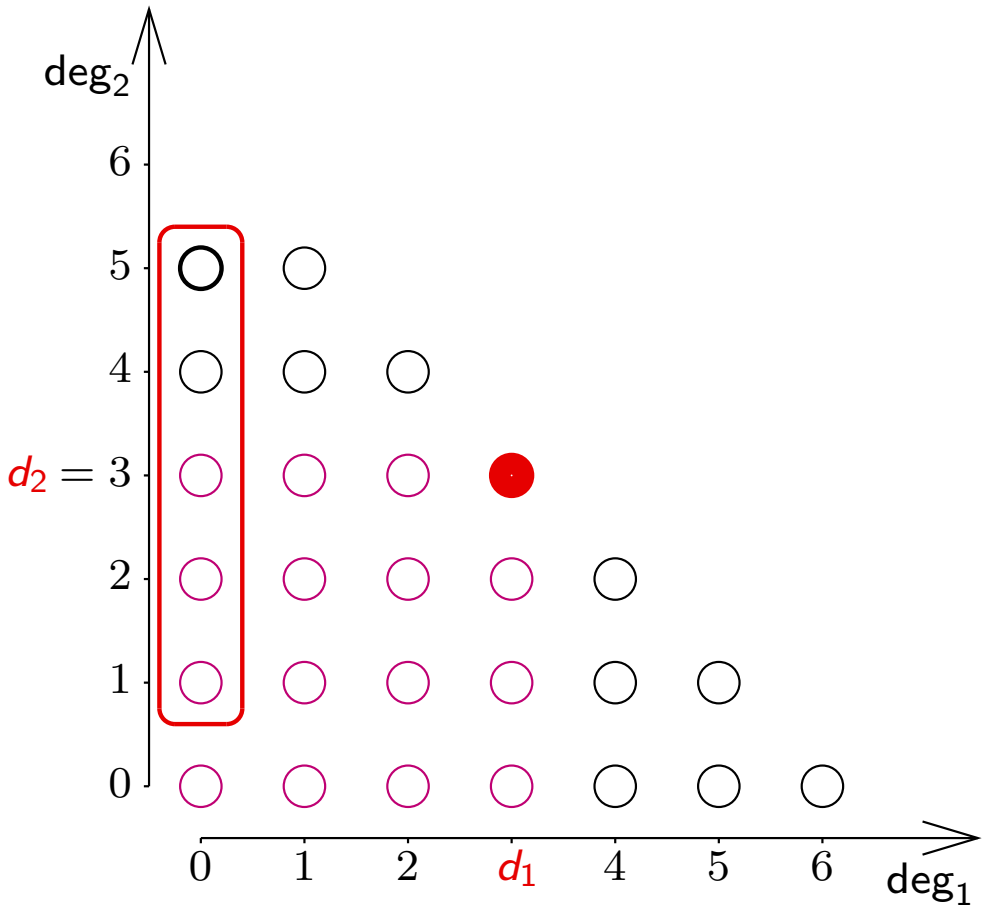
$$+ \quad c \; X^{(0,2)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



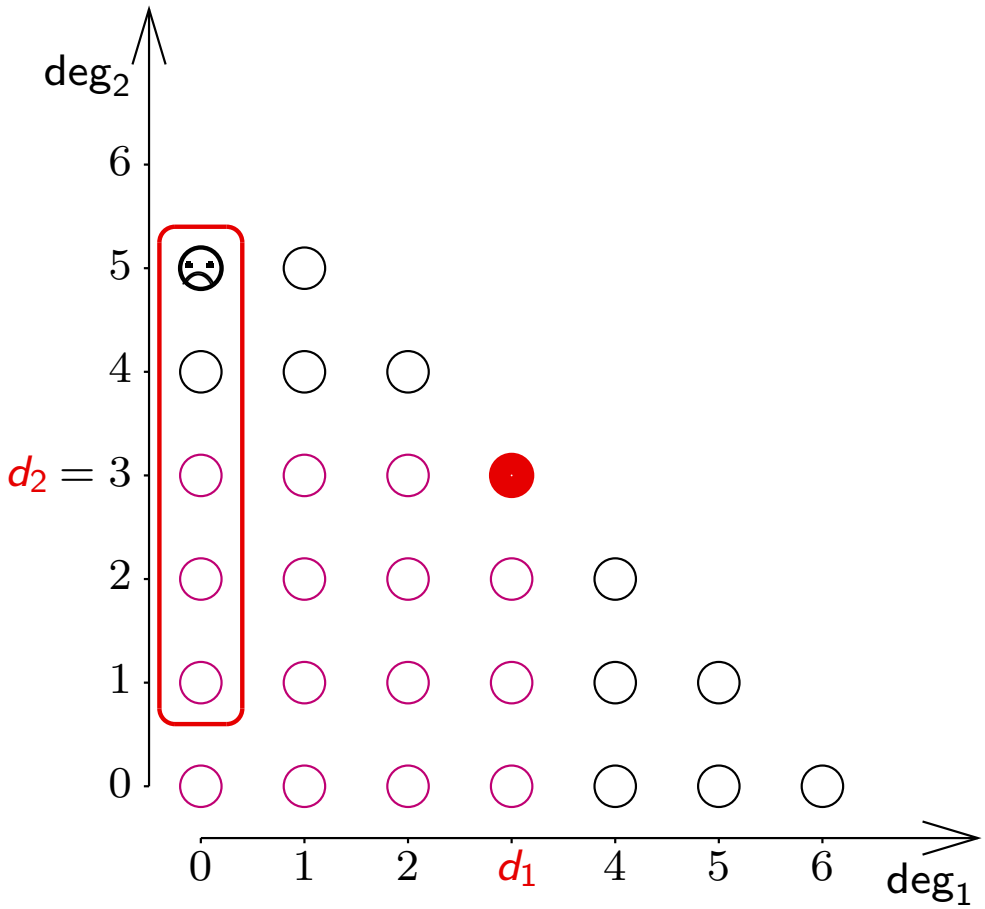
$$+ \quad c\ X^{(0,1)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \quad \equiv 0 \ \text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



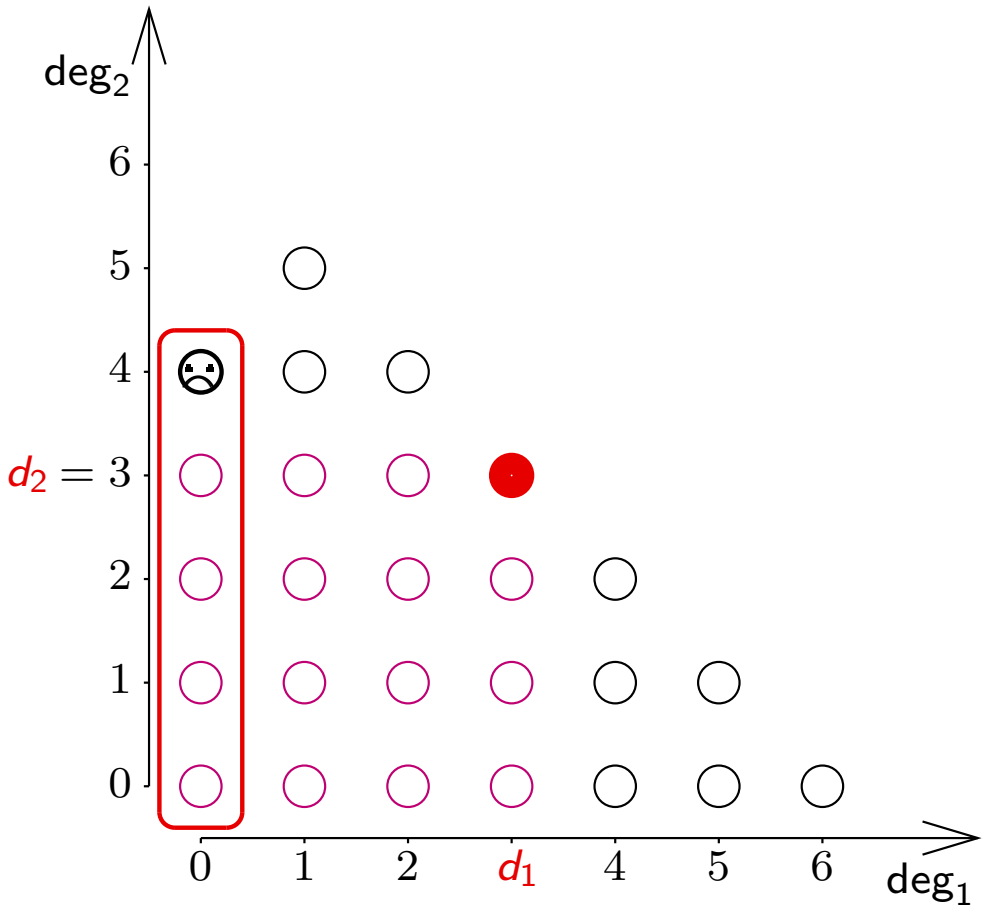
$$+ \quad c \; X^{(0,1)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



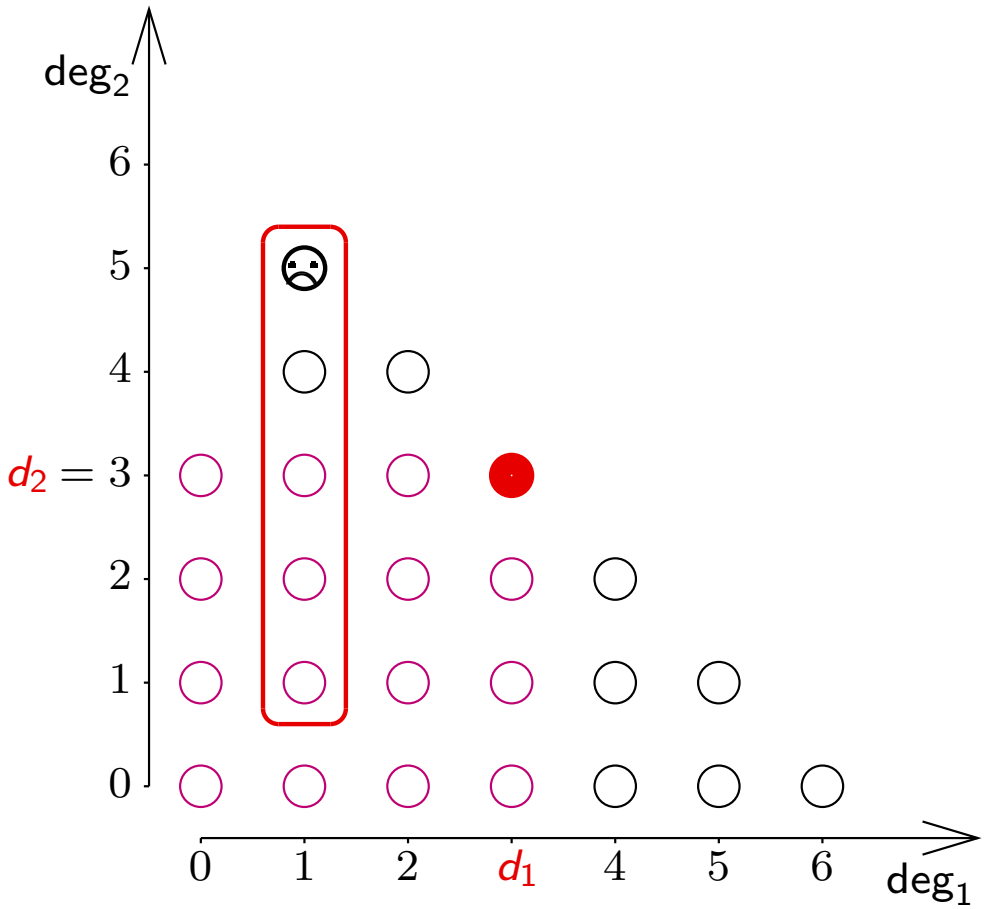
$$+ \quad c \; X^{(0,1)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



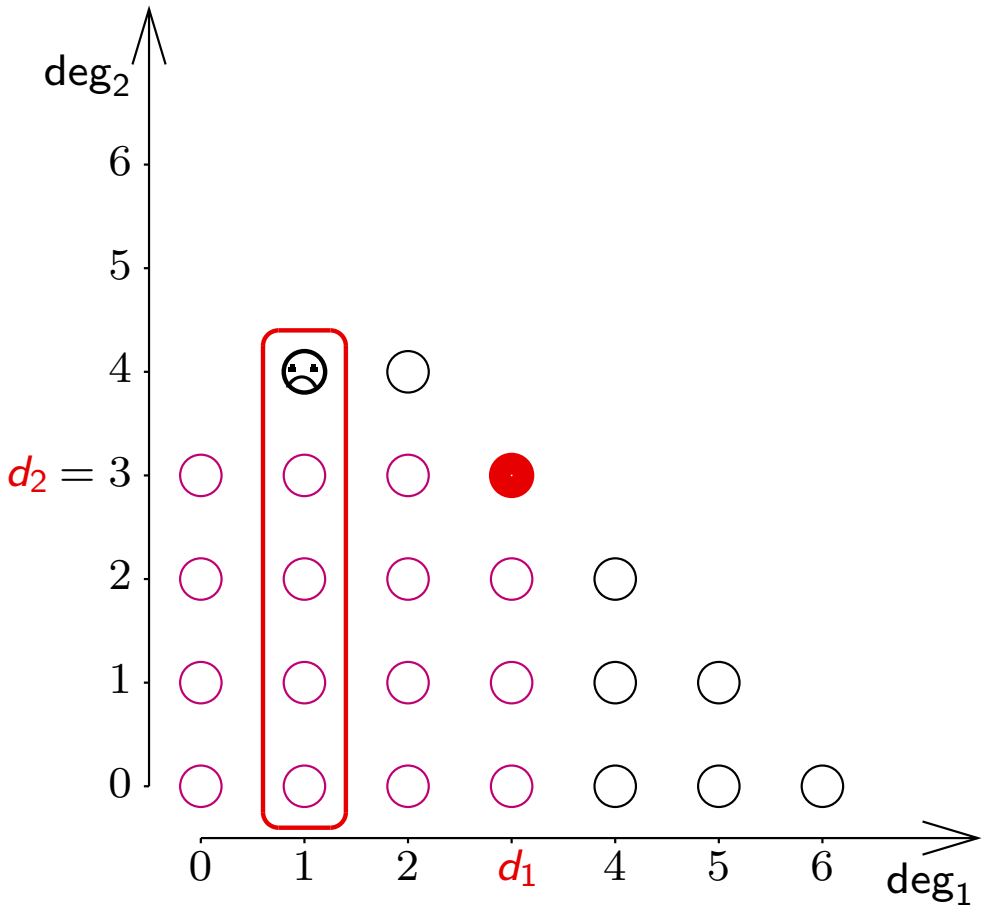
$$+ \quad c \; X^{(0,0)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



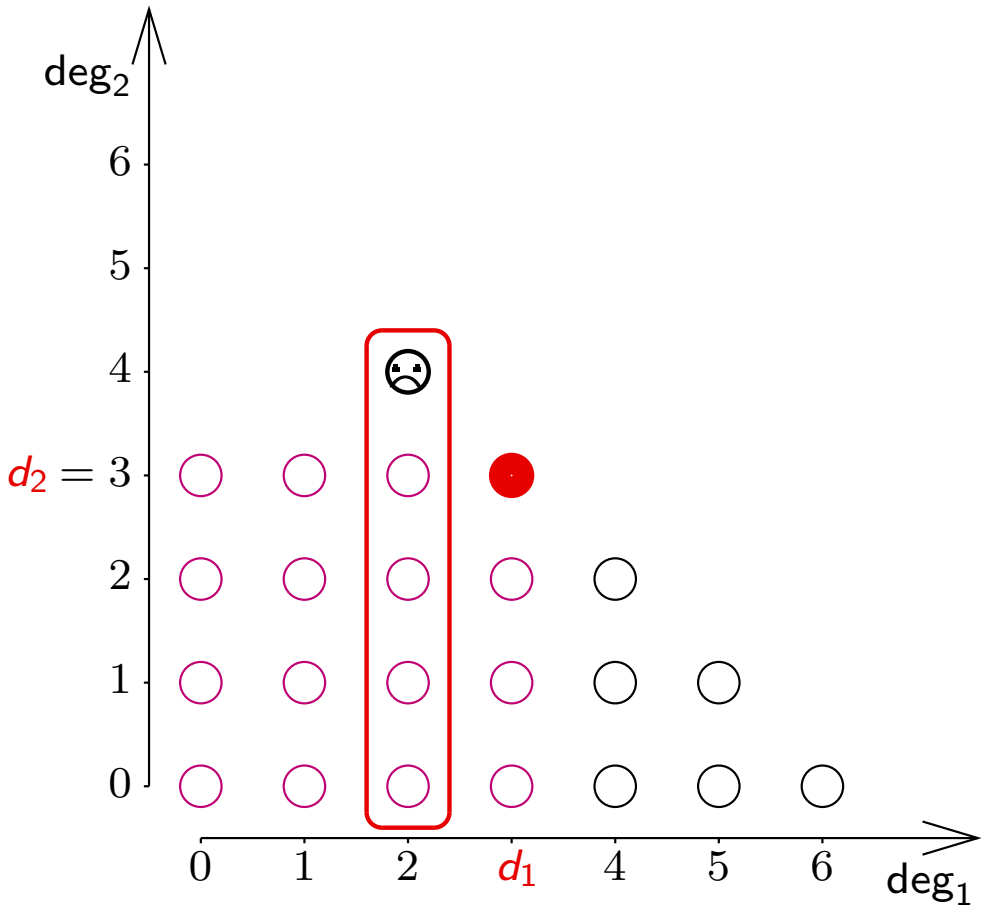
$$+ \quad c \; X^{(1,1)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



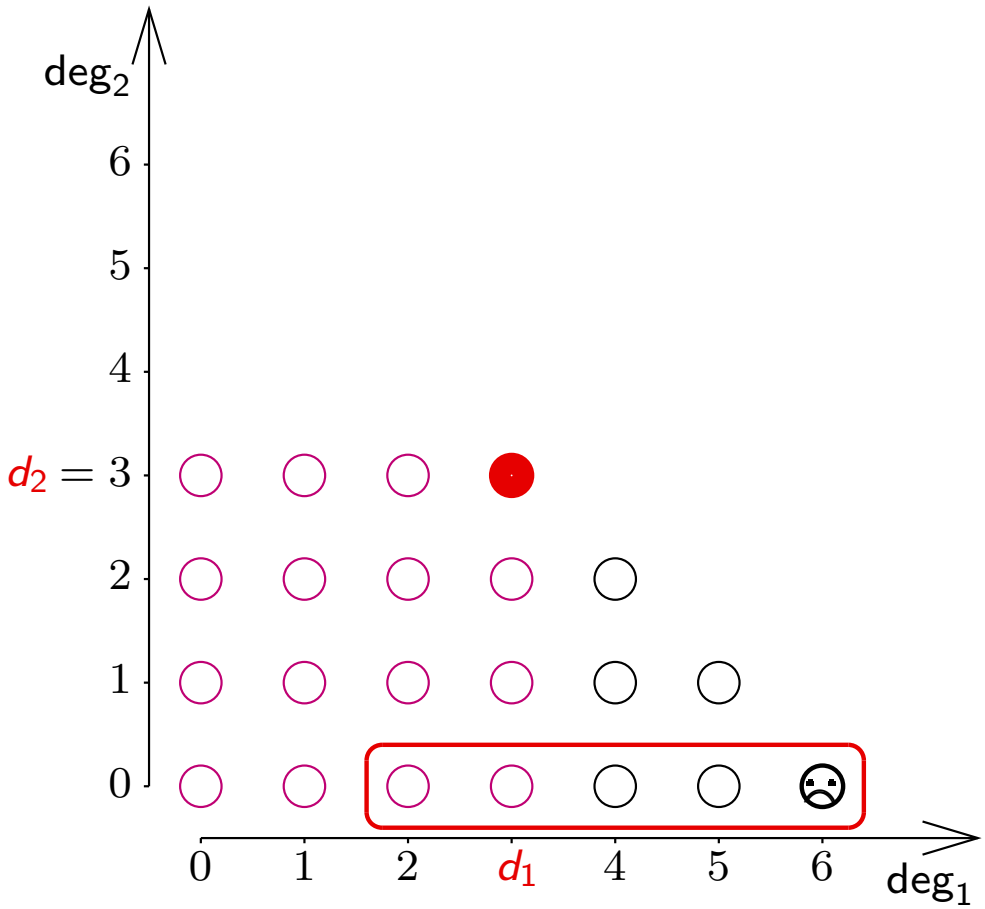
$$+ \quad c \; X^{(1,0)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



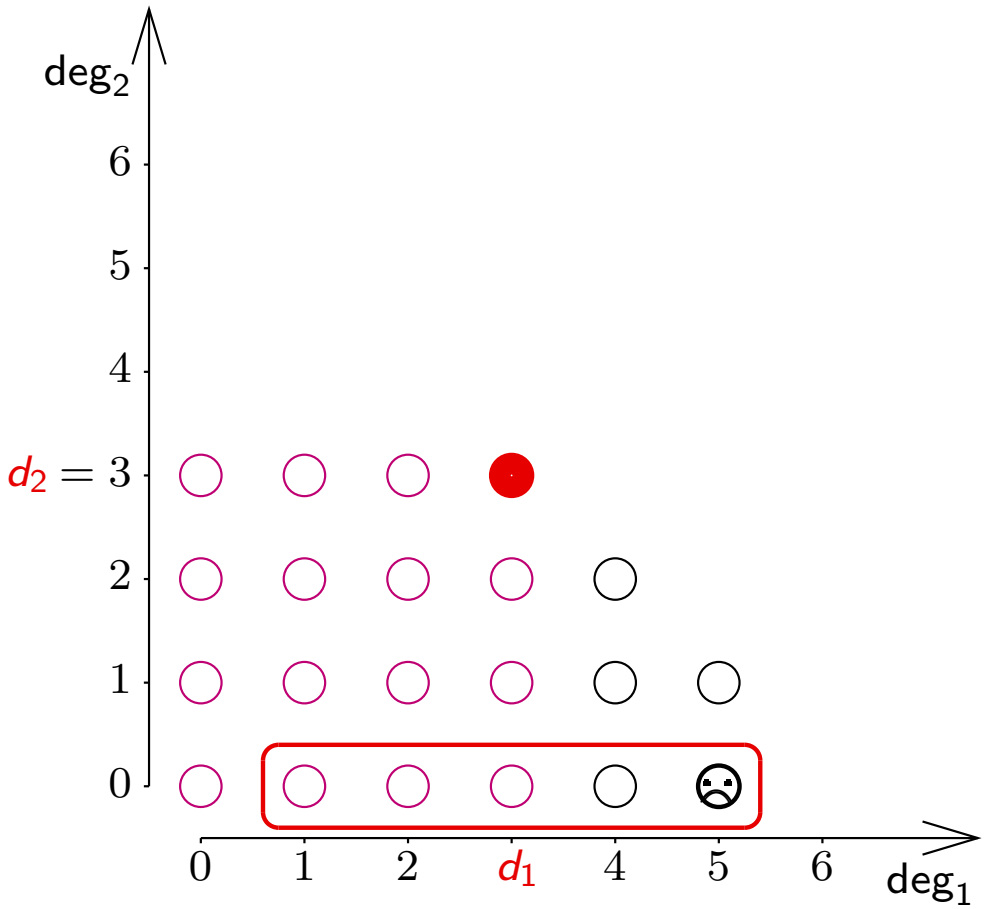
$$+ \quad c \; X^{(2,0)} \prod_{\xi \in \mathfrak{X}_2} (X_2 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



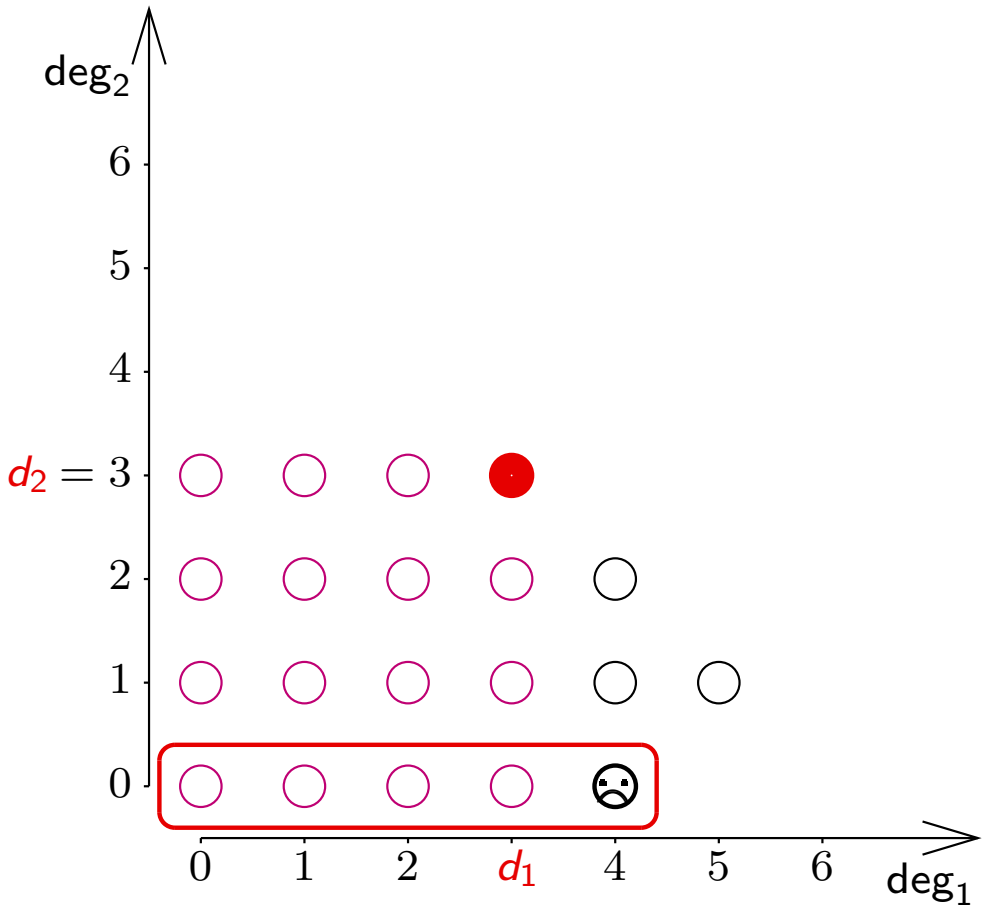
$$+ \quad c \; X^{(2,0)} \prod_{\xi \in \mathfrak{X}_1} (X_1 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



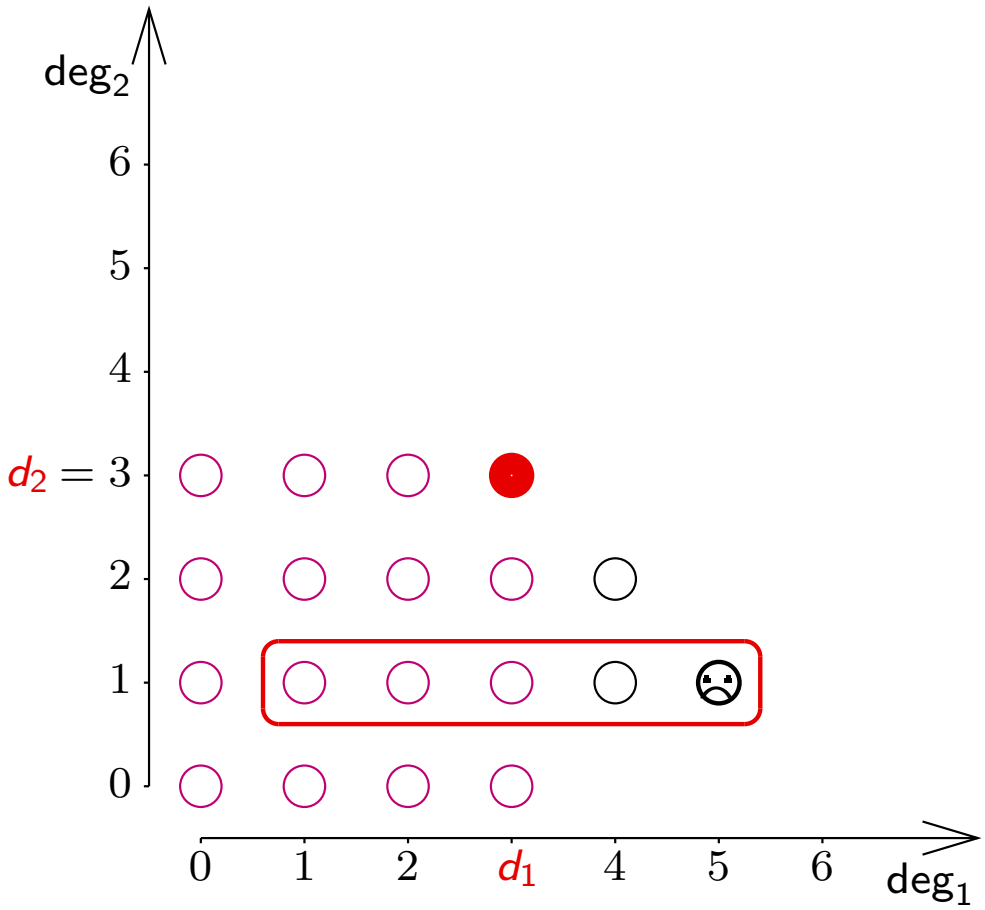
$$+ \quad c \; X^{(1,0)} \prod_{\xi \in \mathfrak{X}_1} (X_1 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



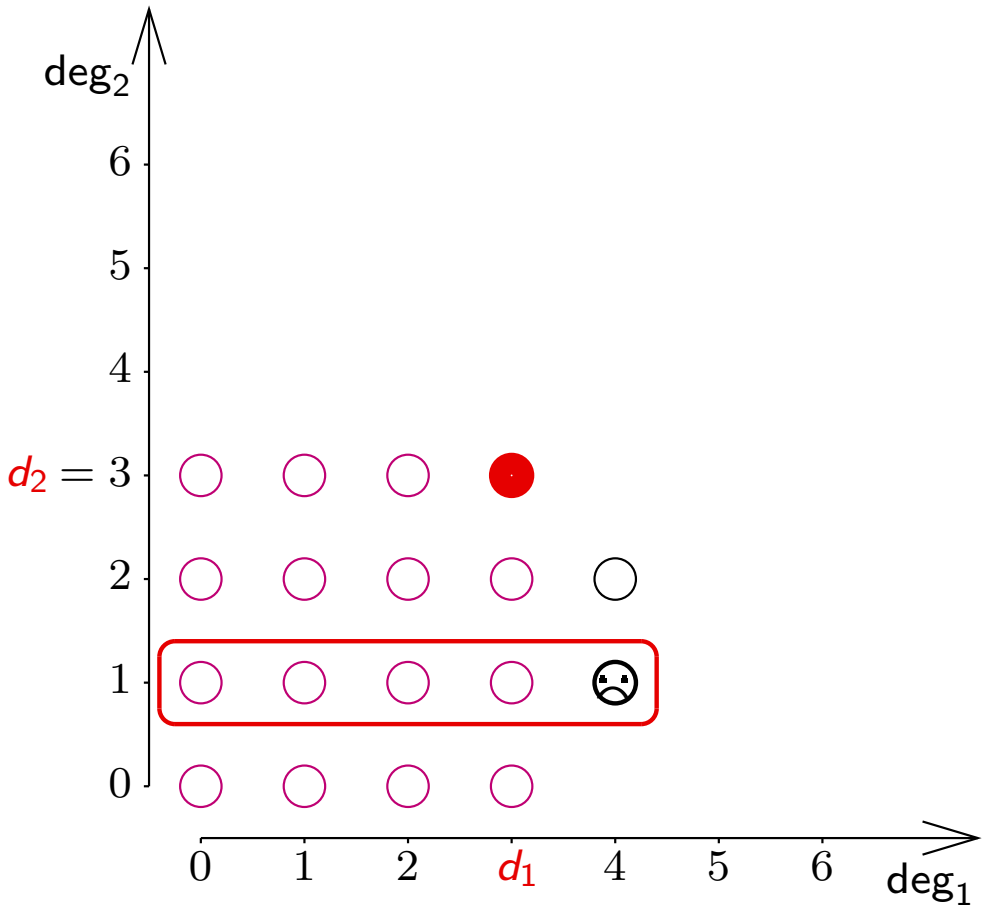
$$+ \quad c \; X^{(0,0)} \prod_{\xi \in \mathfrak{X}_1} (X_1 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



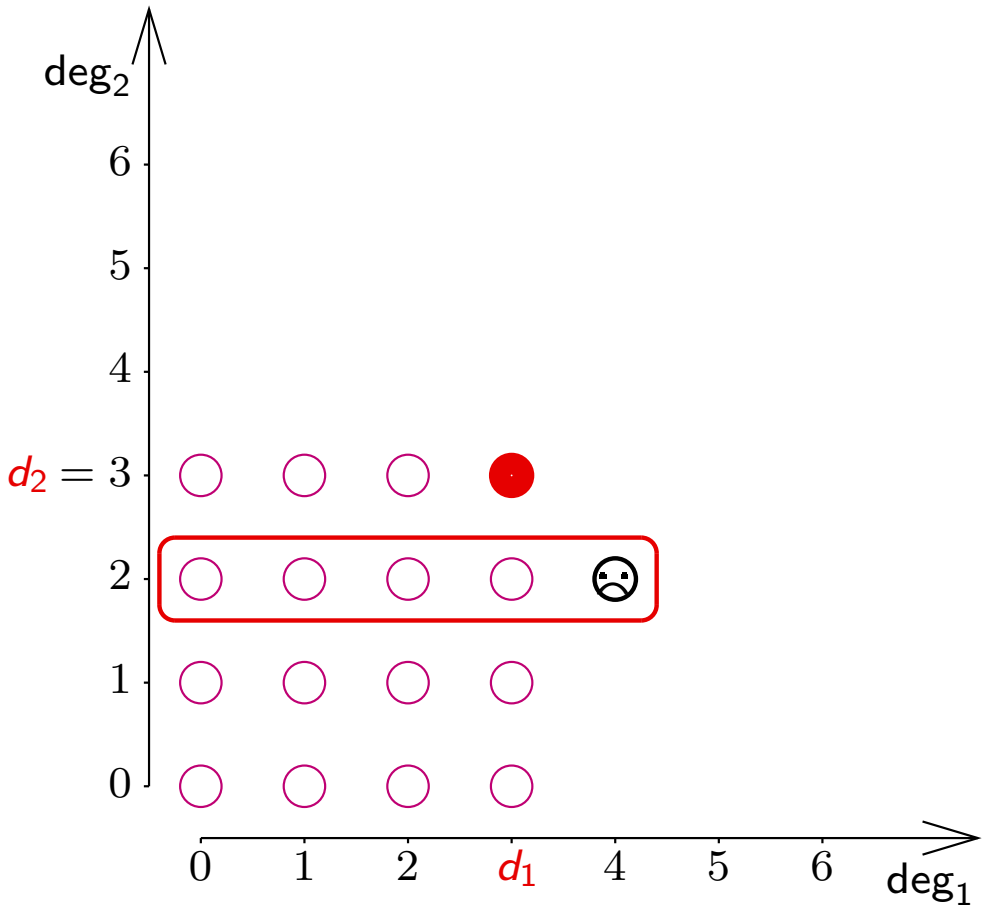
$$+ \quad c \; X^{(1,1)} \prod_{\xi \in \mathfrak{X}_1} (X_1 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



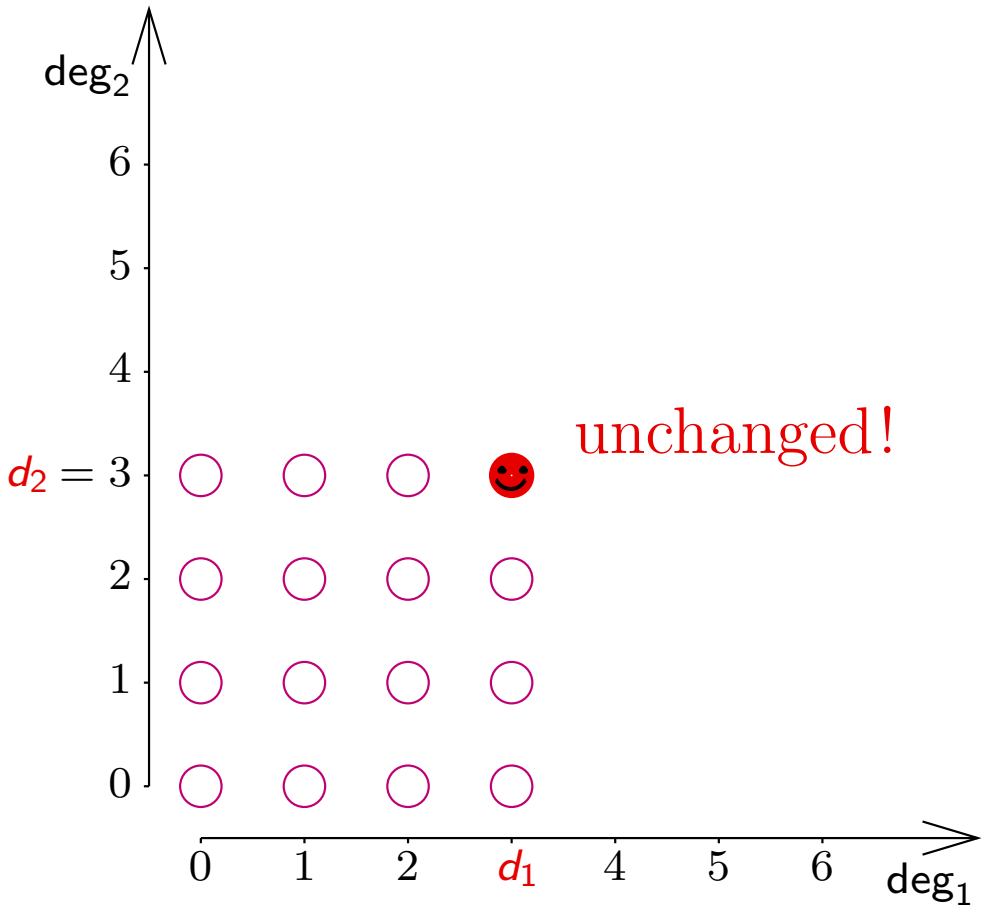
$$+ \quad c \; X^{(0,1)} \prod_{\xi \in \mathfrak{X}_1} (X_1 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



$$+ \quad c \; X^{(0,2)} \prod_{\xi \in \mathfrak{X}_1} (X_1 - \xi) \qquad \equiv 0 \;\text{ on } \mathfrak{X}$$

The transformation $P \longmapsto \longmapsto \cdots \longmapsto P/\mathfrak{X}$:



The trimmed polynomial $P/\mathfrak{X}$.

Specializations of the Quantitative Combinatorial Nullstellensatz

If $\deg(P) \leq \Sigma d$, then $$P_d = \sum_{x \in I} N(x)^{-1} P(x)$$

Let $A \in \mathbb{F}^{m \times n}$, $b \in \mathbb{F}^m$.
If $m \leq \Sigma d$, then $$\mathrm{per}_d(A) = \sum_{x \in I} N(x)^{-1} \overbrace{\prod (Ax - b)}^{\text{Matrix Poly.}}$$

Let d_v denote the indegree of the vertices $v \in V$ of $\vec{G} = (V, \vec{E})$ and let $I_v \subseteq \mathbb{F}$ be a "list of $d_v + 1$ colors" so that the set $I := \prod_{v \in V} I_v$ of potential list colorings of $\vec{G}$ is a d-grid for $d := (d_v)_{v \in V}$, then

$$\pm \underbrace{|EE| \mp |EO|}_{\text{Eulerian Subgraphs}} = \mathrm{per}_d(\underbrace{A(\vec{G})}_{\text{Incidence Matrix}}) = \sum_{x \in I} N(x)^{-1} \overbrace{\prod_{\vec{st} \in \vec{E}} (x_t - x_s)}^{\text{Graph Poly.}}$$

If $\vec{L}$ is the arbitrarily oriented line graph of a planar k-regular graph G and $d_e = k - 1$ for all $e \in E(G) = V(\vec{L})$, then

$$\text{const} \cdot \mathrm{per}_d(A(\vec{L})) = \text{"the number of edge } k\text{-colorings of } G\text{"}$$

Theorem (Alon, Friedland, Kalai)

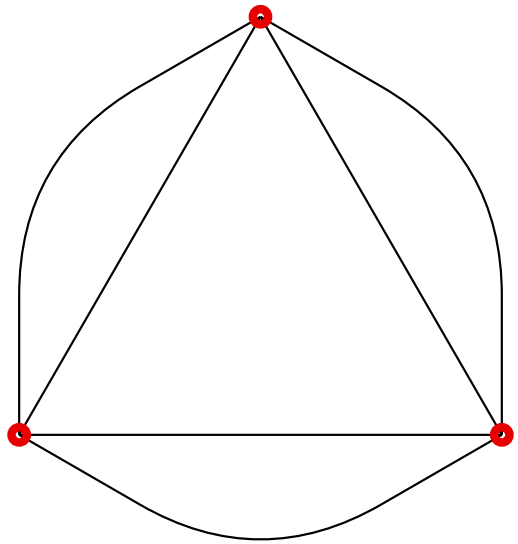
Every loopless 4-regular multigraph plus one edge $G = (V, E \uplus \{e_0\})$ *contains a nontrivial 3-regular subgraph.*

Theorem (Alon, Friedland, Kalai)

Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*

Theorem (Alon, Friedland, Kalai)

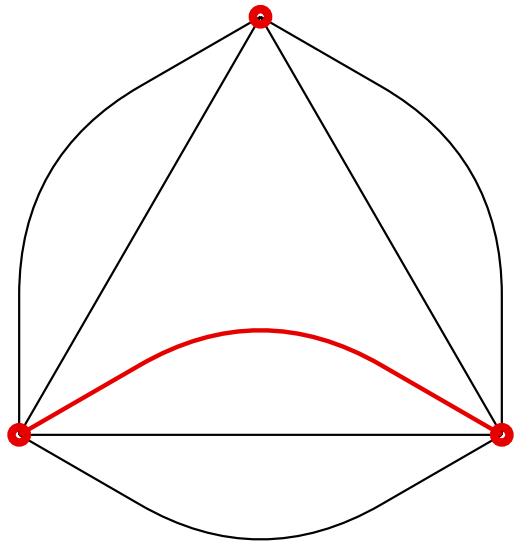
Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*



A 4-regular graph without 3-regular subgraph

Theorem (Alon, Friedland, Kalai)

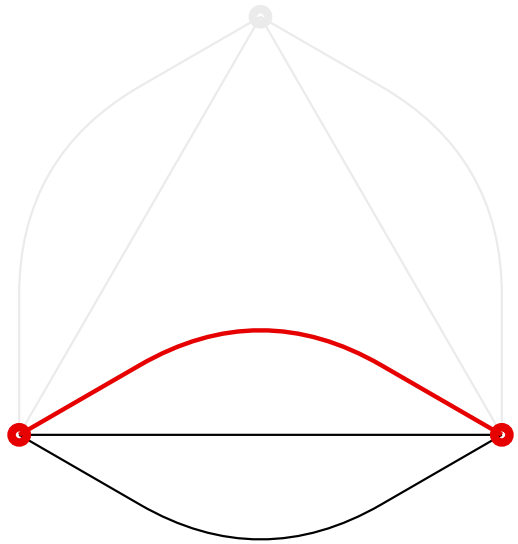
Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*



Extended graph

Theorem (Alon, Friedland, Kalai)

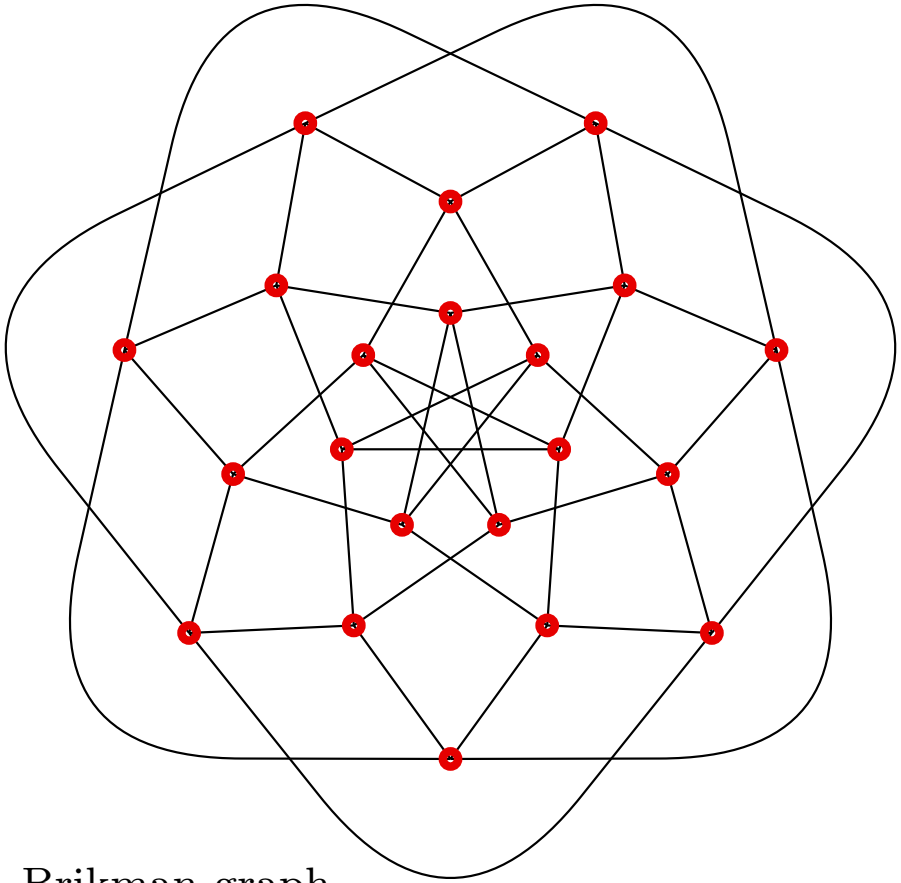
Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*



3-regular subgraph

Theorem (Alon, Friedland, Kalai)

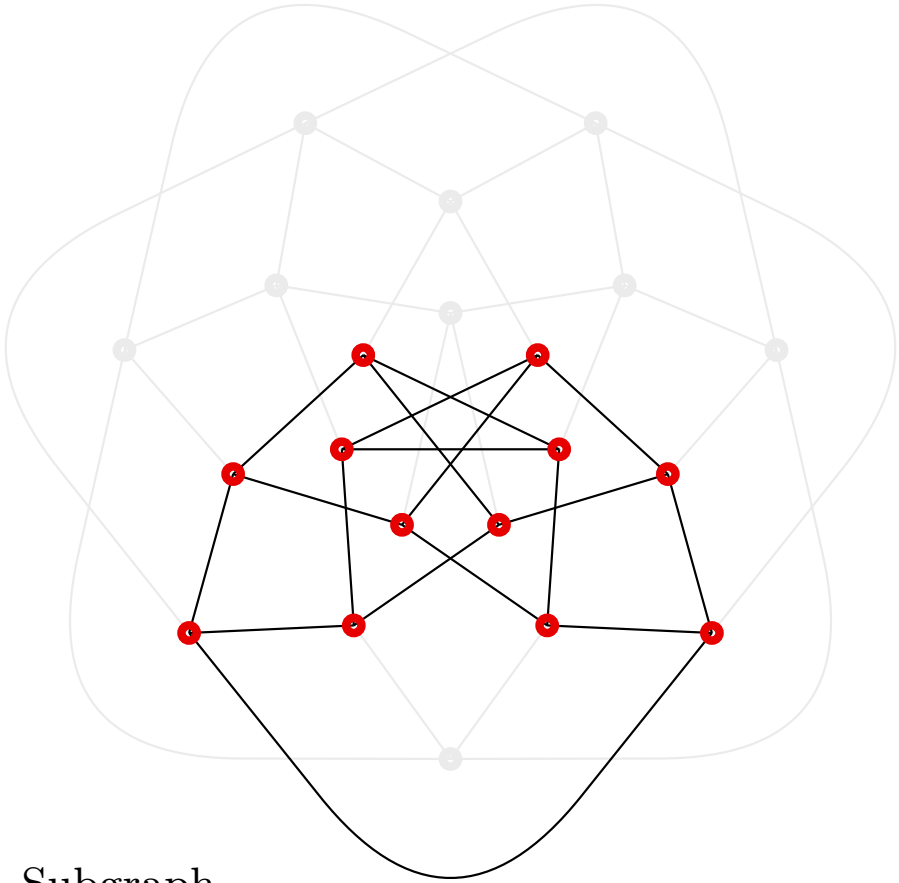
Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*



Brikman graph

Theorem (Alon, Friedland, Kalai)

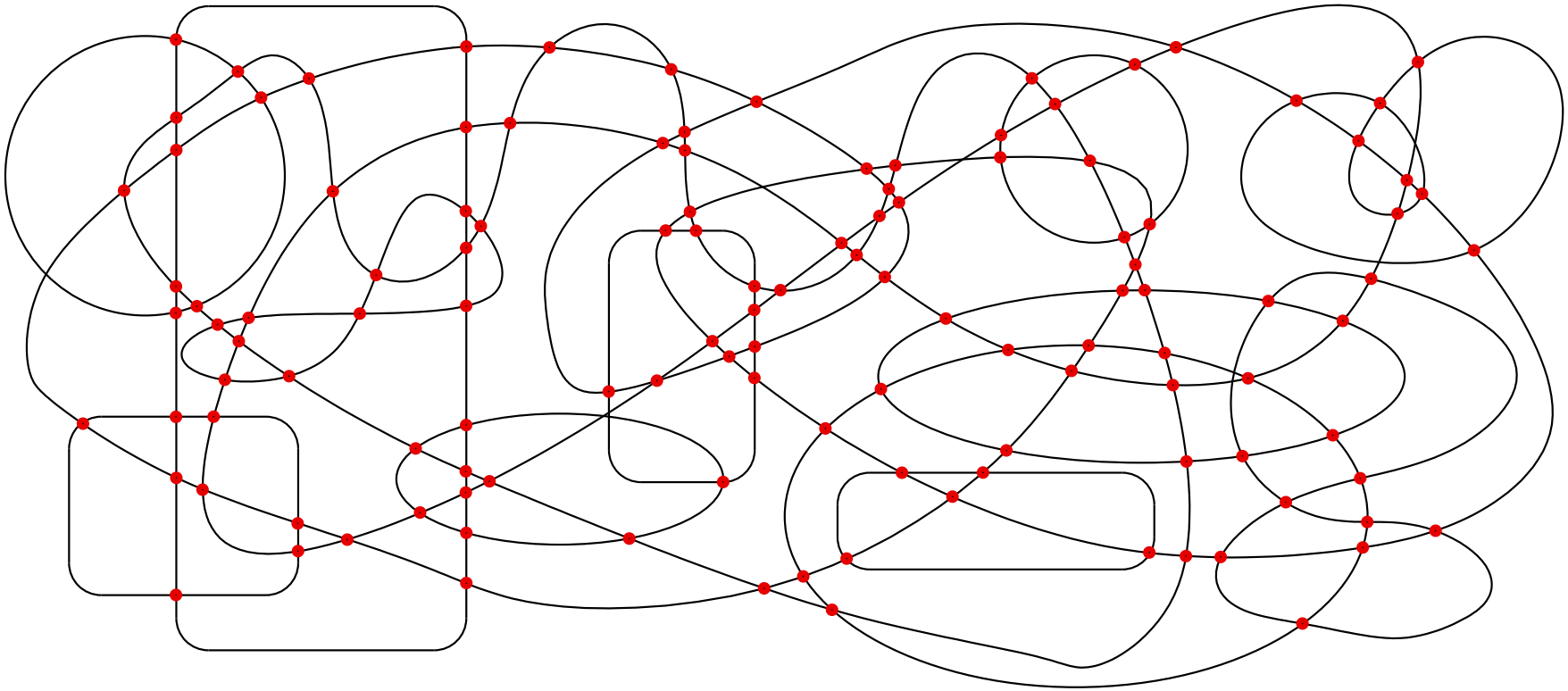
Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*



Subgraph

Theorem (Alon, Friedland, Kalai)

Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*



An other 4-regular graph

Theorem (Alon, Friedland, Kalai)

Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*

I am sure there is one!

Theorem (Alon, Friedland, Kalai)

Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*

Proof.

The subgraphs $H \subseteq \bar{E}$ correspond to the points $x = (x_e)_{e \in \bar{E}}$ of the Boolean grid $I := \{0,1\}^{\bar{E}} \subseteq \mathbb{F}_3^{\bar{E}}$.

$\left(\begin{array}{c} \bar{E} \longleftrightarrow \{1,\ldots,n\} \\ V \longleftrightarrow \{1,\ldots,m\} \end{array} \right)$

Algebraic Solution:

$$P_v := \sum_{e \ni v} X_e \in \mathbb{F}_3[X_e \mid e \in \bar{E}] \quad \text{for all } v \in V.$$

Degree Restriction: $(3-1)\sum_v \deg(P_v) = 2|V| = |E| < |\bar{E}| = \sum_e d_e$.

$$\left.\begin{array}{r} \text{not exactly one} \quad \text{solution} \\ \text{exactly one trivial solution} \end{array}\right\} \text{at least one nontrivial solution!}$$

□

Theorem (Alon, Friedland, Kalai)

Every *loopless 4-regular multigraph plus one edge* ($\bar{E}$) $G = (V, E \uplus \{e_0\})$ *contains a nontrivial 3-regular subgraph.*

extended 4-regular graph

Proof.

The subgraphs $H \subseteq \bar{E}$ correspond to the points $x = (x_e)_{e \in \bar{E}}$ of the Boolean grid $I := \{0,1\}^{\bar{E}} \subseteq \mathbb{F}_3^{\bar{E}}$.

$\left(\begin{array}{c} \bar{E} \longleftrightarrow \{1,\ldots,n\} \\ V \longleftrightarrow \{1,\ldots,m\} \end{array} \right)$

Algebraic Solution:

$$P_v := \sum_{e \ni v} X_e \in \mathbb{F}_3[\, X_e \mid e \in \bar{E}\,] \quad \text{for all } v \in V\,.$$

Degree Restriction: $(3-1)\sum_v \deg(P_v) = 2|V| = |E| < |\bar{E}| = \sum_e d_e$.

not exactly one solution
exactly one trivial solution
} at least one nontrivial solution!

Theorem (Alon, Friedland, Kalai)

Every $\overbrace{\text{loopless 4-regular multigraph plus one edge}}^{\text{extended 4-regular graph}}$ $G = (V, \overbrace{E \uplus \{e_0\}}^{\bar{E}})$ *contains a nontrivial 3-regular subgraph.*

Proof.

The subgraphs $H \subseteq \bar{E}$ correspond to the points $x = (x_e)_{e \in \bar{E}}$ of the Boolean grid $I := \{0,1\}^{\bar{E}} \subseteq \mathbb{F}_3^{\bar{E}}$.

$\left(\begin{array}{c} \bar{E} \longleftrightarrow \{1,\ldots,n\} \\ V \longleftrightarrow \{1,\ldots,m\} \end{array} \right)$

Algebraic Solution:

$$P_v := \sum_{e \ni v} X_e \in \mathbb{F}_3[\, X_e \mid e \in \bar{E}\,] \quad \text{for all } v \in V\,.$$

Degree Restriction: $(3-1)\sum_v \deg(P_v) = 2|V| = |E| < |\bar{E}| = \sum_e d_e$.

not exactly one solution
exactly one trivial solution
} at least one nontrivial solution!

Theorem (Alon, Friedland, Kalai)

Every *loopless 4-regular multigraph plus one edge* ($G = (V, \bar{E} = E \uplus \{e_0\})$) *contains a nontrivial 3-regular subgraph.*

Proof.

The subgraphs $H \subseteq \bar{E}$ correspond to the points $x = (x_e)_{e \in \bar{E}}$ of the Boolean grid $I := \{0,1\}^{\bar{E}} \subseteq \mathbb{F}_3^{\bar{E}}$.

$\left(\begin{array}{c} \bar{E} \longleftrightarrow \{1,\ldots,n\} \\ V \longleftrightarrow \{1,\ldots,m\} \end{array} \right)$

Algebraic Solution:

$$P_v := \sum_{e \ni v} X_e \in \mathbb{F}_3[\, X_e \mid e \in \bar{E}\,] \quad \text{for all } v \in V\,.$$

Degree Restriction: $(3-1)\sum_v \deg(P_v) = 2|V| = |E| < |\bar{E}| = \sum_e d_e$.

not exactly one solution
exactly one trivial solution
} **at least one nontrivial solution!**

□

Theorem (Non-uniqueness Theorem)

Let R *be a commutative ring with* $1 \neq 0$ *and* $P \in R[X_1, X_2, \ldots, X_n]$ *.*
If $\deg(P) < n$ *then*

$$\left|\left\{ x \in \{0,1\}^n \mid P(x) \neq 0 \right\}\right| \neq 1 \ .$$

Theorem (Version of Warning's Theorem)

Let $\mathbb{F}_q$ *be the field of order* q *and* $P_1, \ldots, P_m \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ *.*
If $(q-1)\sum_{i=1}^{m} \deg(P_i) < n$ *then*

$$\left|\left\{ x \in \{0,1\}^n \mid P_1(x) = \cdots = P_m(x) = 0 \right\}\right| \neq 1 \ .$$

Proof.

Define $P := \prod_{i=1}^{m}(1 - P_i^{q-1})$ and apply the Non-uniqueness Theorem. □

Theorem (Non-uniqueness Theorem)

Let R *be a commutative ring with* $1 \neq 0$ *and* $P \in R[X_1, X_2, \ldots, X_n]$ *.*
If $\deg(P) < n$ *then*

$$\left|\left\{ x \in \{0,1\}^n \mid P(x) \neq 0 \right\}\right| \neq 1 \ .$$

Theorem (Version of Warning's Theorem)

Let $\mathbb{F}_q$ *be the field of order* q *and* $P_1, \ldots, P_m \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ *.*
If $(q-1)\sum_{i=1}^{m} \deg(P_i) < n$ *then*

$$\left|\left\{ x \in \{0,1\}^n \mid P_1(x) = \cdots = P_m(x) = 0 \right\}\right| \neq 1 \ .$$

Proof.

Define $P := \prod_{i=1}^{m}(1 - P_i^{q-1})$ and apply the Non-uniqueness Theorem. □

Theorem (Non-uniqueness Theorem)

Let R *be a commutative ring with* $1 \neq 0$ *and* $P \in R[X_1, X_2, \ldots, X_n]$ *.*
If $\deg(P) < n$ *then*

$$\left|\left\{ x \in \{0,1\}^n \mid P(x) \neq 0 \right\}\right| \neq 1 \ .$$

Theorem (Version of Warning's Theorem)

Let $\mathbb{F}_q$ *be the field of order* q *and* $P_1, \ldots, P_m \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ *.*
If $(q-1)\sum_{i=1}^{m} \deg(P_i) < n$ *then*

$$\left|\left\{ x \in \{0,1\}^n \mid P_1(x) = \cdots = P_m(x) = 0 \right\}\right| \neq 1 \ .$$

Proof.

Define $P := \prod_{i=1}^{m}(1 - P_i^{q-1})$ and apply the Non-uniqueness Theorem. □

Theorem (Non-existence of Lagrange Functions)

Let $P \in \mathbb{Z}_k[X_1, \ldots, X_n]$ *. If* k *is not prime, and* $(k, n) \neq (4, 1)$ *, then*

$$\left|\{\, x \in \mathbb{Z}_k^n \mid P(x) \neq 0 \,\}\right| \neq 1 \,.$$

$$-\tfrac{1}{8}X^4+\tfrac{3}{4}X^3-\tfrac{7}{8}X^2-\tfrac{3}{4}X+1:\ \mathbb{Z}\longrightarrow\mathbb{Q}$$

$$=\ -3\binom{X}{4}+\binom{X}{2}-\binom{X}{1}+\binom{X}{0}:\ \mathbb{Z}\longrightarrow\mathbb{Z}$$

$$\mathbb{Z}\longrightarrow\mathbb{Z}_9$$

3-periodic:

$$-3\binom{X}{4}+\binom{X}{2}-\binom{X}{1}+\binom{X}{0}:\ \mathbb{Z}_3\longrightarrow\mathbb{Z}_9$$

P(x+3)=P(x)

$$f:\mathbb{Z}\longrightarrow\mathbb{Z}_9 \text{ is 3-periodic} \iff f:\mathbb{Z}_3\longrightarrow\mathbb{Z}_9$$

$$\mathbb{Z}_9^{\mathbb{Z}_3}\subseteq\mathbb{Z}_9^{\mathbb{Z}_6}\subseteq\mathbb{Z}_9^{\mathbb{Z}}$$

$$-\tfrac{1}{8}X^4+\tfrac{3}{4}X^3-\tfrac{7}{8}X^2-\tfrac{3}{4}X+1:\ \mathbb{Z}\longrightarrow\mathbb{Q}$$

$$=\ -3\binom{X}{4}+\binom{X}{2}-\binom{X}{1}+\binom{X}{0}:\ \mathbb{Z}\longrightarrow\mathbb{Z}$$

$$-\bar{3}\binom{X}{4}+\bar{1}\binom{X}{2}-\bar{1}\binom{X}{1}+\bar{1}\binom{X}{0}:\ \mathbb{Z}\longrightarrow\mathbb{Z}_9 \qquad \text{3-periodic}$$

$$\underbrace{-\bar{3}\binom{X}{4}+\bar{1}\binom{X}{2}-\bar{1}\binom{X}{1}+\bar{1}\binom{X}{0}}_{\in\mathbb{Z}_9\binom{X}{\mathbb{Z}_3}\subseteq\mathbb{Z}_9\binom{X}{\mathbb{Z}}}:\ \underbrace{\mathbb{Z}_3\longrightarrow\mathbb{Z}_9}_{\in\mathbb{Z}_9^{\mathbb{Z}_3}\subseteq\mathbb{Z}_9^{\mathbb{Z}}} \qquad \bar{a}:=a+9\mathbb{Z}$$

$$\mathbb{Z}_9\binom{X}{\mathbb{Z}_3}\ \hookrightarrow\ \mathbb{Z}_9^{\mathbb{Z}_3} \quad \text{is injective.}$$

$$\mathbb{Z}_9\binom{X}{\mathbb{Z}_3}\ =\ \{f\in\mathbb{Z}_9^{\mathbb{Z}_3}\mid f \text{ arises from a } \hat{f}\in\mathbb{Q}[X]\}$$

Good news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{p^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^\alpha}} \quad \text{for primes } p\,.$$

Any function $\mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arises from a polynomial, in particular the Lagrange Function L, which maps nonzeros to zero and zero to one. If $\beta = 1$ then $L\colon \mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_p$ has degree $p^\alpha - 1$.

Bad news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{q^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^0}} = \mathbb{Z}_{p^\beta} \quad \text{for different primes } p \text{ and } q\,.$$

Only constant functions $\mathbb{Z}_{q^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arise from a polynomial.

The *general case* $\mathbb{Z}_r\binom{X}{\mathbb{Z}_s}$ is a certain mixture of these cases.

Good news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{p^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^\alpha}} \quad \text{for primes } p\,.$$

Any function $\mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arises from a polynomial, in particular the Lagrange Function L, which maps nonzeros to zero and zero to one.

If $\beta = 1$ then $L\colon \mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_p$ has degree $p^\alpha - 1$.

Bad news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{q^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^0}} = \mathbb{Z}_{p^\beta} \quad \text{for different primes } p \text{ and } q\,.$$

Only constant functions $\mathbb{Z}_{q^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arise from a polynomial.

The *general case* $\mathbb{Z}_r\binom{X}{\mathbb{Z}_s}$ is a certain mixture of these cases.

Good news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{p^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^\alpha}} \quad \text{for primes } p\,.$$

Any function $\mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arises from a polynomial, in particular the Lagrange Function L, which maps nonzeros to zero and zero to one.
If $\beta = 1$ then $L\colon \mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_p$ has degree $p^\alpha - 1$.

Bad news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{q^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^0}} = \mathbb{Z}_{p^\beta} \quad \text{for different primes } p \text{ and } q\,.$$

Only constant functions $\mathbb{Z}_{q^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arise from a polynomial.

The *general case* $\mathbb{Z}_r\binom{X}{\mathbb{Z}_s}$ is a certain mixture of these cases.

Good news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{p^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^\alpha}} \quad \text{for primes } p\,.$$

Any function $\mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arises from a polynomial, in particular the Lagrange Function L, which maps nonzeros to zero and zero to one.
If $\beta = 1$ then $L\colon \mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_p$ has degree $p^\alpha - 1$.

Bad news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{q^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^0}} = \mathbb{Z}_{p^\beta} \quad \text{for different primes } p \text{ and } q\,.$$

Only constant functions $\mathbb{Z}_{q^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arise from a polynomial.

The *general case* $\mathbb{Z}_r\binom{X}{\mathbb{Z}_s}$ is a certain mixture of these cases.

Good news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{p^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^\alpha}} \quad \text{for primes } p\,.$$

Any function $\mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arises from a polynomial, in particular the Lagrange Function L, which maps nonzeros to zero and zero to one.
If $\beta = 1$ then $L\colon \mathbb{Z}_{p^\alpha} \longrightarrow \mathbb{Z}_p$ has degree $p^\alpha - 1$.

Bad news:

$$\mathbb{Z}_{p^\beta}\binom{X}{\mathbb{Z}_{q^\alpha}} = (\mathbb{Z}_{p^\beta})^{\mathbb{Z}_{p^0}} = \mathbb{Z}_{p^\beta} \quad \text{for different primes } p \text{ and } q\,.$$

Only constant functions $\mathbb{Z}_{q^\alpha} \longrightarrow \mathbb{Z}_{p^\beta}$ arise from a polynomial.

The *general case* $\mathbb{Z}_r\binom{X}{\mathbb{Z}_s}$ is a certain mixture of these cases.

Theorem (Quantitative Combinatorial Nullstellensatz)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$, $d_j := |I_j| - 1$, $d := (d_j)$.
For polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}[X_1, \ldots, X_n]$ *with* $\deg(P) \leq \Sigma_j d_j$,

$$P_d = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x)P(x) \ , \quad \text{with certain } M(x) \in \mathbb{F} \backslash 0 \, .$$

Theorem (Generalized Quantitative Combinatorial Nullstellensatz)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of* p, $d_j := |I_j| - 1$, $d := (d_j)$.
For integer valued polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{Q}[X_1, \ldots, X_n]$ *with* $\deg(P) \leq \Sigma_j d_j$, *which we view as map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}_p$,

$$\underbrace{((p-1)!)^n P_d}_{\in \mathbb{Z}} + p\mathbb{Z} = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x)P(x) \ , \quad \text{with certain } M(x) \in \mathbb{Z}_p \backslash 0 \, .$$

Theorem (Quantitative Combinatorial Nullstellensatz)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$, $d_j := |I_j| - 1$, $d := (d_j)$.
For polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}[X_1, \ldots, X_n]$ *with* $\deg(P) \leq \Sigma_j d_j$,

$$P_d = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x)P(x) \ , \quad \text{with certain } M(x) \in \mathbb{F} \setminus 0 \, .$$

Theorem (Generalized Quantitative Combinatorial Nullstellensatz)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of* p, $d_j := |I_j| - 1$, $d := (d_j)$.
For integer valued polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{Q}[X_1, \ldots, X_n]$ *with* $\deg(P) \leq \Sigma_j d_j$, *which we view as map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}_p$,

$$\underbrace{((p-1)!)^n P_d}_{\in \mathbb{Z}} + p\mathbb{Z} = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x)P(x) \ , \quad \text{with certain } M(x) \in \mathbb{Z}_p \setminus 0 \, .$$

Theorem (Quantitative Combinatorial Nullstellensatz)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$, $d_j := |I_j| - 1$, $d := (d_j)$.
For polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{F}[X_1, \ldots, X_n]$ *with* $\deg(P) \leq \Sigma_j d_j$,

$$P_d = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x) P(x) \ , \quad \text{with certain } M(x) \in \mathbb{F} \backslash 0 \, .$$

Theorem (Generalized Quantitative Combinatorial Nullstellensatz)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of* p, $d_j := |I_j| - 1$, $d := (d_j)$.
For integer valued polynomials $P = \sum_{\delta \in \mathbb{N}^n} P_\delta X^\delta \in \mathbb{Q}[X_1, \ldots, X_n]$ *with* $\deg(P) \leq \Sigma_j d_j$, *which we view as map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}_p$,

$$\underbrace{((p-1)!)^n P_d}_{\in \mathbb{Z}} + p\mathbb{Z} = \sum_{x \in I_1 \times I_2 \times \cdots \times I_n} M(x) P(x) \ , \quad \text{with certain } M(x) \in \mathbb{Z}_p \backslash 0 \, .$$

Theorem (Non-uniqueness Theorem)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$ *and* $P \in \mathbb{F}[X_1, X_2, \ldots, X_n]$.
If $\deg(P) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\{\, x \in I_1 \times I_2 \times \cdots \times I_n \;\vert\; P(x) \neq 0 \,\}\right| \neq 1 \ .$$

Theorem (Generalized Non-uniqueness Theorem)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of* p . *Let* $P \in \mathbb{Q}[X_1, \ldots, X_n]$ *be integer valued. We view view* P *as map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}_p$.
If $\deg(P) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\{\, x \in I_1 \times I_2 \times \cdots \times I_n \;\vert\; P(x) \neq 0 \,\}\right| \neq 1 \ .$$

Theorem (Non-uniqueness Theorem)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$ *and* $P \in \mathbb{F}[X_1, X_2, \ldots, X_n]$. *If* $\deg(P) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\{\, x \in I_1 \times I_2 \times \cdots \times I_n \;\mid\; P(x) \neq 0 \,\}\right| \neq 1 \ .$$

Theorem (Generalized Non-uniqueness Theorem)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of* p . *Let* $P \in \mathbb{Q}[X_1, \ldots, X_n]$ *be integer valued. We view view* P *as map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}_p$.

If $\deg(P) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\{\, x \in I_1 \times I_2 \times \cdots \times I_n \;\mid\; P(x) \neq 0 \,\}\right| \neq 1 \ .$$

Theorem (Non-uniqueness Theorem)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a field* $\mathbb{F}$ *and* $P \in \mathbb{F}[X_1, X_2, \ldots, X_n]$.
If $\deg(P) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\{\, x \in I_1 \times I_2 \times \cdots \times I_n \;\mid\; P(x) \neq 0 \,\}\right| \neq 1 \ .$$

Theorem (Generalized Non-uniqueness Theorem)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of* p . *Let* $P \in \mathbb{Q}[X_1, \ldots, X_n]$ *be integer valued. We view view* P *as map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}_p$.
If $\deg(P) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\{\, x \in I_1 \times I_2 \times \cdots \times I_n \;\mid\; P(x) \neq 0 \,\}\right| \neq 1 \ .$$

Theorem (Version of Warning's Theorem)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a the finite field* $\mathbb{F}_q$ *, and let* $P_1, P_2, \ldots, P_m \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ *.*
If $(q-1)\sum_{i=1}^{m} \deg(P_i) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\left\{ x \in I_1 \times I_2 \times \cdots \times I_n \;\middle|\; P_1(x) = \cdots = P_m(x) = 0 \right\}\right| \neq 1 \ .$$

Theorem (Generalized Version of Warning's Theorem)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of a given prime* p *, and let* $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$ *and* $0 < k_1, \ldots, k_m \in \mathbb{Z}$ *.*
If $\sum_{i=1}^{m} (p^{k_i} - 1) \deg(P_i) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\left\{ x \in \mathfrak{X} \;\middle|\; \forall\, i\colon\ p^{k_i} \,\middle|\, P_i(x) \right\}\right| \neq 1 \ .$$

Theorem (Version of Warning's Theorem)

Let $I_1, I_2, \ldots, I_n$ *be finite subsets of a the finite field* $\mathbb{F}_q$ *, and let* $P_1, P_2, \ldots, P_m \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ *.*
If $(q-1)\sum_{i=1}^{m} \deg(P_i) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\left\{ x \in I_1 \times I_2 \times \cdots \times I_n \;\middle|\; P_1(x) = \cdots = P_m(x) = 0 \right\}\right| \neq 1 \ .$$

Theorem (Generalized Version of Warning's Theorem)

For $j = 1, \ldots, n$ *let* $I_j \subseteq \mathbb{Z}$ *be such that the distances* $x_2 - x_1$ *between any two elements of* I_j *is not a multiple of a given prime* p *, and let* $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$ *and* $0 < k_1, \ldots, k_m \in \mathbb{Z}$ *.*
If $\sum_{i=1}^{m}(p^{k_i} - 1)\deg(P_i) < |I_1| + |I_2| + \cdots + |I_n| - n$ *then*

$$\left|\left\{ x \in \mathfrak{X} \;\middle|\; \forall\, i\colon\ p^{k_i} \,\middle|\, P_i(x) \right\}\right| \neq 1 \ .$$

Theorem (Olson's Theorem for primes p)

Any sequence of $(p-1)m+1$ elements of $\mathbb{Z}_p^m$ contains a subsequence that sums to zero.

Theorem (Generalized Olson Theorem)

Any sequence of $1+\sum_i(p^{k_i}-1)$ elements of $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_m}}$ contains a subsequence that sums to zero.

Conjecture (Alon, Friedland, Kalai)

For any integer $k \geq 2$, any sequence of $(k-1)n+1$ elements of $\mathbb{Z}_k^n$ contains a subsequence that sums to zero.

Theorem (Olson's Theorem for primes p)

Any sequence of $(p-1)m+1$ elements of $\mathbb{Z}_p^m$ contains a subsequence that sums to zero.

Theorem (Generalized Olson Theorem)

Any sequence of $1+\sum_i(p^{k_i}-1)$ elements of $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_m}}$ contains a subsequence that sums to zero.

Conjecture (Alon, Friedland, Kalai)

For any integer $k \geq 2$, any sequence of $(k-1)n+1$ elements of $\mathbb{Z}_k^n$ contains a subsequence that sums to zero.

Theorem (Olson's Theorem for primes p)

Any sequence of $(p-1)m+1$ elements of $\mathbb{Z}_p^m$ contains a subsequence that sums to zero.

Theorem (Generalized Olson Theorem)

Any sequence of $1+\sum_i(p^{k_i}-1)$ elements of $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_m}}$ contains a subsequence that sums to zero.

Conjecture (Alon, Friedland, Kalai)

For any integer $k \geq 2$, any sequence of $(k-1)n+1$ elements of $\mathbb{Z}_k^n$ contains a subsequence that sums to zero.

Theorem (Alon, Friedland, Kalai)

For prime powers q holds the following: Every loopless $(2q-2)$-regular multigraph plus one edge contains a nontrivial q-regular subgraph.

Conjecture (Alon, Friedland, Kalai).

This holds for any integer $q \geq 2$.

Theorem (Alon, Friedland, Kalai)

For prime powers q holds the following: Every loopless $(2q-2)$-regular multigraph plus one edge contains a nontrivial q-regular subgraph.

Conjecture (Alon, Friedland, Kalai).

This holds for any integer $q \geq 2$.

Assume

$$f \in \mathbb{Z}_{12}\binom{X}{\mathbb{Z}_{50}} \ .$$

Then

$$\phi \circ f \circ \vartheta^{-1} \in (\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{5^0})\binom{X_1,\ X_2,\ X_3}{\mathbb{Z}_{2^1} \times \mathbb{Z}_{3^0} \times \mathbb{Z}_{5^2}} = \mathbb{Z}_4^{\mathbb{Z}_2} \times \mathbb{Z}_3^{\mathbb{Z}_1} \times \mathbb{Z}_1^{\mathbb{Z}_{25}} \cong \mathbb{Z}_4^2 \times \mathbb{Z}_3$$

with the Chinese Reminder Isomorphisms

$$\phi\colon \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{5^0} \qquad \text{and} \qquad \vartheta\colon \mathbb{Z}_{50} \longrightarrow \mathbb{Z}_{2^1} \times \mathbb{Z}_{3^0} \times \mathbb{Z}_{5^2} \ .$$

Hence,

$$\phi \circ f \circ \vartheta^{-1} = (g, c, 0) \in \mathbb{Z}_4^{\mathbb{Z}_2} \times \mathbb{Z}_3^{\{0\}} \times \{0\}^{\mathbb{Z}_{25}} \ .$$

It follows that

$$f = 9g + 4c = -3g + 4c \ ,$$

with a 2-periodic $g\colon \mathbb{Z} \longrightarrow \{0, 1, 2, 3\} \subseteq \mathbb{Z}_{12}$ and a constant $c \in \{0, 1, 2\} \subseteq \mathbb{Z}_{12}$. In other words,

$$f\colon \mathbb{Z} \longrightarrow \mathbb{Z}_{12} \ \text{ is 2-periodic and } \ f(1) - f(0) \in \{0, 3, 6, 9\} \subseteq \mathbb{Z}_{12} \ .$$

Thank You!