AN APPLICATION OF ALGEBRAIC GEOMETRY TO A COMBINATORIAL PROBLEM

Jarkko Kari, Michal Szabados

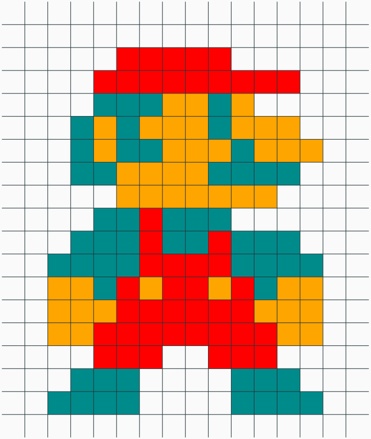
November 19-22, 2015

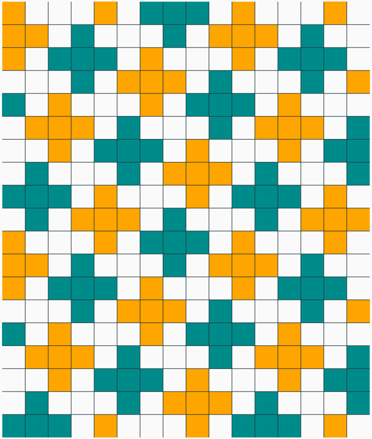
University of Turku, Finland

NIVAT'S CONJECTURE

Let $\mathcal{A}$ be a finite set.

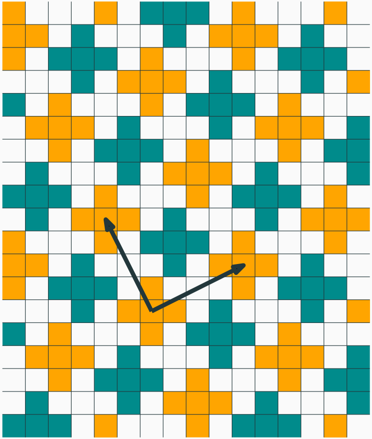
Coloring of an infinite square grid: a function $\mathbb{Z}^2 \to \mathcal{A}$

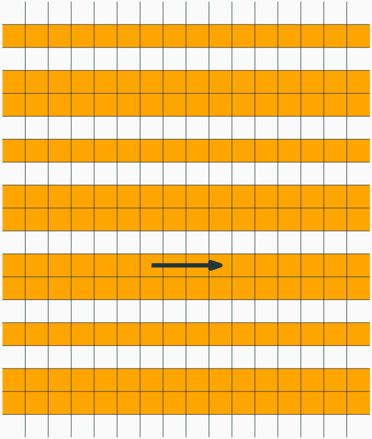




Periodic coloring: $\exists\, \mathbf{v} \in \mathbb{Z}^2$ non-zero vector such that

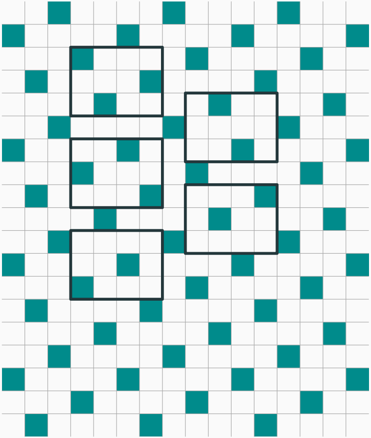
$$\forall\, \mathbf{u} \in \mathbb{Z}^2: \quad c_{\mathbf{u}} = c_{\mathbf{u}+\mathbf{v}}$$

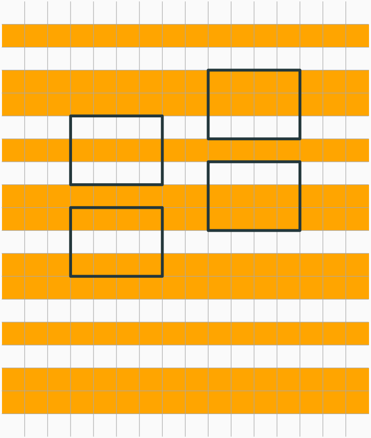




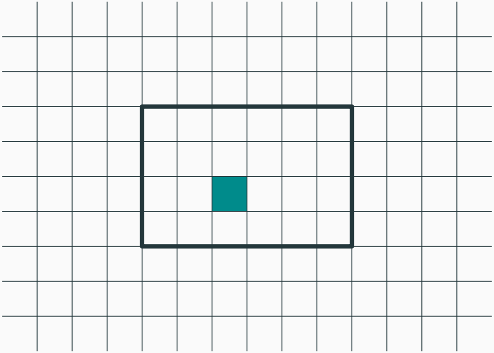
Rectangle complexity $P(m, n)$:

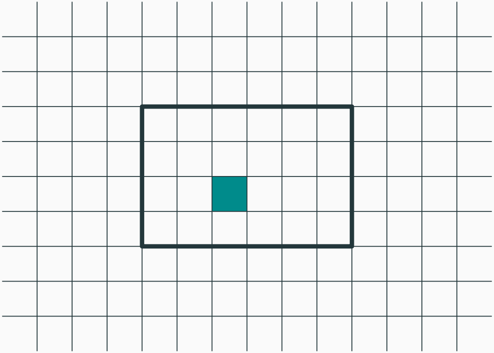
# of distinct patterns in blocks $m \times n$





NIVAT'S CONJECTURE





Nivat's Conjecture [Nivat, 1997]:

$$\text{non-periodic coloring} \quad \Rightarrow \quad \forall m, n \colon P(m,n) \geq mn + 1$$

Nivat's Conjecture [Nivat, 1997]:

$$\text{non-periodic coloring} \quad \Rightarrow \quad \forall m, n\colon\ P(m, n) \geq mn + 1$$

Known results [Van Cyr, Bryna Kra 2013]:

- non-periodic coloring $\quad \Rightarrow \quad \forall m, n\colon\ P(m, n) > mn/2$
- non-periodic coloring $\quad \Rightarrow \quad \forall m\colon\ P(m, 3) \geq 3m + 1$

Nivat's Conjecture [Nivat, 1997]:

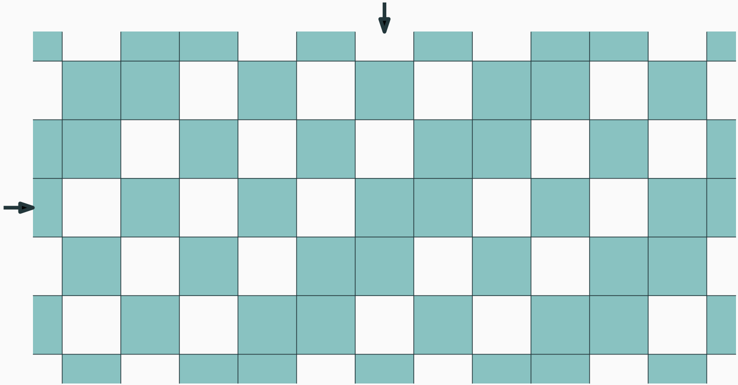
$$\text{non-periodic coloring} \quad \Rightarrow \quad \forall m, n\colon\ P(m, n) \geq mn + 1$$

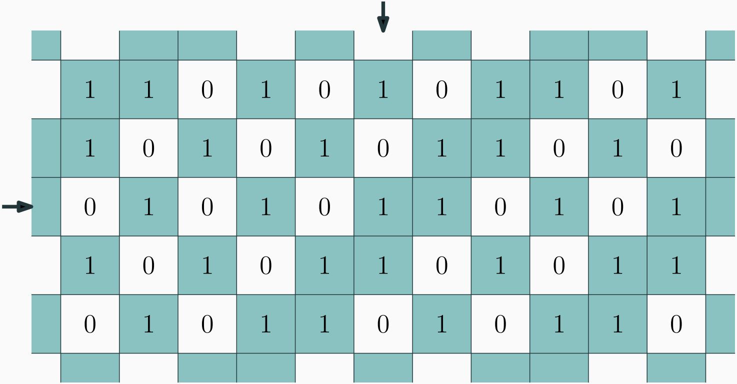
Theorem [K., S. 2015]:

$$\text{non-periodic coloring}$$
$$\Downarrow$$
$$\text{for all but finitely many pairs m,n:}\ P(m, n) \geq mn + 1$$

OUR METHOD

FORMAL POWER SERIES




1 1 0 1 0 1 0 1 1 0 1
1 0 1 0 1 0 1 1 0 1 0
0 1 0 1 0 1 1 0 1 0 1
1 0 1 0 1 1 0 1 0 1 1
0 1 0 1 1 0 1 0 1 1 0

FORMAL POWER SERIES

$x^{-5}y^2$	$x^{-4}y^2$	0	$x^{-2}y^2$	0	y^2	0	x^2y^2	x^3y^2	0	x^5y^2
$x^{-5}y$	0	$x^{-3}y$	0	$x^{-1}y$	0	xy	x^2y	0	x^4y	0
0	x^{-4}	0	x^{-2}	0	1	x	0	x^3	0	x^5
$x^{-5}y^{-1}$	0	$x^{-3}y^{-1}$	0	$x^{-1}y^{-1}$	y^{-1}	0	x^2y^{-1}	0	x^4y^{-1}	x^5y^{-1}
0	$x^{-4}y^{-2}$	0	$x^{-2}y^{-2}$	$x^{-1}y^{-2}$	0	xy^{-2}	0	x^3y^{-2}	x^4y^{-2}	0

At position (i, j) : $c_{ij}x^iy^j$

$$x^{-5}y^2 + x^{-4}y^2 + 0 + x^{-2}y^2 + 0 + y^2 + 0 + x^2y^2 + x^3y^2 + 0 + x^5y^2$$

$$x^{-5}y + 0 + x^{-3}y + 0 + x^{-1}y + 0 + xy + x^2y + 0 + x^4y + 0$$

$$0 + x^{-4} + 0 + x^{-2} + 0 + 1 + x + 0 + x^3 + 0 + x^5$$

$$x^{-5}y^{-1} + 0 + x^{-3}y^{-1} + 0 + x^{-1}y^{-1} + y^{-1} + 0 + x^2y^{-1} + 0 + x^4y^{-1} + x^5y^{-1}$$

$$0 + x^{-4}y^{-2} + 0 + x^{-2}y^{-2} + x^{-1}y^{-2} + 0 + xy^{-2} + 0 + x^3y^{-2} + x^4y^{-2} + 0$$

$$\sum_{(i,j)\in\mathbb{Z}^2} c_{ij}x^iy^j$$

Configuration: formal power series over $\mathbb{C}$

$$c(x, y) = \sum_{(i,j)\in\mathbb{Z}^2} c_{ij} x^i y^j$$

integral: coefficients from $\mathbb{Z}$

finitary: finitely many distinct coefficients

Configuration: formal power series $c \in \mathbb{C}[[X^{\pm 1}]]$

$$c(X) = \sum_{\mathbf{v} \in \mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$$

GROWN-UP NOTATION

integral: coefficients from $\mathbb{Z}$

finitary: finitely many distinct coefficients

Configuration: formal power series $c \in \mathbb{C}[[X^{\pm 1}]]$

$$c(X) = \sum_{\mathbf{v} \in \mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$$

integral: coefficients from $\mathbb{Z}$

finitary: finitely many distinct coefficients

$$\boxed{\text{coloring} \quad \longleftrightarrow \quad \text{finitary integral configuration}}$$

Configuration: formal power series over $\mathbb{C}$

$$c(x, y) = \sum_{(i,j)\in\mathbb{Z}^2} c_{ij} x^i y^j$$

Question: What happens if $c(x, y)$ is multiplied by $x^a y^b$?

Configuration: formal power series over $\mathbb{C}$

$$c(X) = \sum_{\mathbf{v} \in \mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$$

GROWN-UP NOTATION

Question: What happens if c is multiplied by $X^{\mathbf{u}}$?

Answer: The coloring translates by the vector $\mathbf{u}$!

Configuration: formal power series over $\mathbb{C}$

$$c(X) = \sum_{\mathbf{v} \in \mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$$

Question: What happens if c is multiplied by $X^{\mathbf{u}}$?

Answer: The coloring translates by the vector $\mathbf{u}$!

Observe: Multiplication by a polynomial $\equiv$ linear combination of translates

$$\left(\sum_{i=1}^{n} a_i X^{\mathbf{u}_i} \right) c = \sum_{i=1}^{n} a_i \left(X^{\mathbf{u}_i} c \right)$$

Configuration: formal power series over $\mathbb{C}$

$$c(X) = \sum_{\mathbf{v}\in\mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$$

Question: What happens if c is multiplied by $X^{\mathbf{u}}$?

Answer: The coloring translates by the vector $\mathbf{u}$!

Observe: Configuration is periodic iff $\exists\, \mathbf{u} \neq 0$:

$$\begin{aligned} & X^{\mathbf{u}} c = c \\ \Leftrightarrow \quad & (X^{\mathbf{u}} - 1)c = 0 \end{aligned}$$

ANNIHILATING POLYNOMIALS

$$\boxed{\mathrm{Ann}(c) = \left\{ f(x,y) \in \mathbb{C}[x,y] \;\middle|\; f(x,y)c(x,y) = 0 \right\}}$$

GROWN-UP NOTATION

$$\boxed{\mathrm{Ann}(c) = \{\, f \in \mathbb{C}[X] \mid fc = 0 \,\}}$$

- **Annihilator ideal:** $\mathrm{Ann}(c)$
- **Annihilator polynomial:** $f \in \mathbb{C}[X]$ such that $fc = 0$
- **Observe:** c is periodic iff for some non-zero $\mathbf{v} \in \mathbb{Z}^d$

$$X^{\mathbf{v}} - 1 \in \mathrm{Ann}(c)$$

Lemma: If exist m, n such that $P(m, n) \leq mn$, then $\mathrm{Ann}(c) \neq \{0\}$.

Proof. Linear algebra.

Theorem: Let c be a finitary integral configuration with $\mathrm{Ann}(c) \neq \{0\}$. Then $\exists \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^d$ such that*

$$(X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1) \in \mathrm{Ann}(c).$$

Proof. Hilbert's nullstellensatz.

Theorem: Let c be a two-dimensional finitary integral configuration. Then $\mathrm{Ann}(c)$ is a radical ideal.

Proof. Classification of prime ideals of $\mathbb{C}[x, y]$.

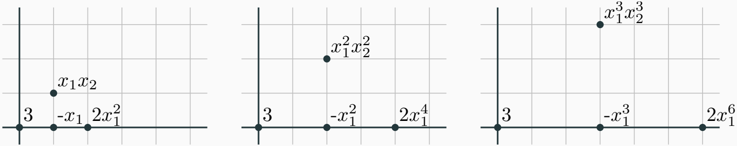
LET'S DO SOME MATH!

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Definition: Denote $f(X) = \sum_{i=1}^{n} a_i X^{\mathbf{v}_i}$, then

$$f(X^p) := \sum_{i=1}^{n} a_i X^{p\mathbf{v}_i}$$



Plot of $f(X)$, $f(X^2)$ and $f(X^3)$ for the polynomial

$$f(X) = f(x_1, x_2) = 3 - x_1 + 2x_1^2 + x_1x_2.$$

LEMMA 1

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Proof:

- $f^p(X) \equiv f(X^p) \pmod p$ because $(x+y)^p \equiv x^p + y^p \pmod p$

LEMMA 1

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Proof:

- $f^p(X) \equiv f(X^p) \pmod{p}$
- $0 \equiv f(X^p)c(X) \pmod{p}$

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Proof:

- $f^p(X) \equiv f(X^p) \pmod{p}$
- $0 \equiv f(X^p)c(X) \pmod{p}$
- coefficients of RHS are bounded by $c_{absmax} \sum |a_i|$

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Proof:

- $f^p(X) \equiv f(X^p) \pmod p$
- $0 \equiv f(X^p)c(X) \pmod p$
- coefficients of RHS are bounded by $c_{absmax} \sum |a_i|$
- choose p larger

LEMMA 1

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Proof:

- $f^p(X) \equiv f(X^p) \pmod p$
- $0 \equiv f(X^p)c(X) \pmod p$
- coefficients of RHS are bounded by $c_{\text{absmax}} \sum |a_i|$
- choose p larger

Lemma: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then, for large enough primes p, also $f(X^p)$ annihilates c.

Proof:

- $f^p(X) \equiv f(X^p) \pmod p$
- $0 \equiv f(X^p)c(X) \pmod p$
- coefficients of RHS are bounded by $c_{\text{absmax}} \sum |a_i|$
- choose p larger

Can be generalized to:

Lemma 1: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Then there exists $r \in \mathbb{N}$ such that also $f(X^{kr+1})$ annihilates c for $k \in \mathbb{N}_0$.

Lemma 2. Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Denote $f = \sum a_{\mathbf{v}} X^{\mathbf{v}}$ and $\mathrm{supp}(f) = \{ \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \}$. Define

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

where r is as in Lemma 1 and $\mathbf{v}_0 \in \mathrm{supp}(f)$ arbitrary. Then $g(Z) = 0$ for any common root $Z \in \mathbb{C}^d$ of $\mathrm{Ann}(c)$.

Lemma 2. Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Denote $f = \sum a_{\mathbf{v}} X^{\mathbf{v}}$ and $\operatorname{supp}(f) = \{ \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \}$. Define

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

where r is as in Lemma 1 and $\mathbf{v}_0 \in \operatorname{supp}(f)$ arbitrary. Then $g(Z) = 0$ for any common root $Z \in \mathbb{C}^d$ of $\operatorname{Ann}(c)$.

Proof.

- Fix $Z = (z_1, \ldots, z_d) \in \mathbb{C}^d$ a root of $\operatorname{Ann}(c)$.

Lemma 2. Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Denote $f = \sum a_{\mathbf{v}} X^{\mathbf{v}}$ and $\operatorname{supp}(f) = \{ \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \}$. Define

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

where r is as in Lemma 1 and $\mathbf{v}_0 \in \operatorname{supp}(f)$ arbitrary. Then $g(Z) = 0$ for any common root $Z \in \mathbb{C}^d$ of $\operatorname{Ann}(c)$.

Proof.

- Fix $Z = (z_1, \ldots, z_d) \in \mathbb{C}^d$ a root of $\operatorname{Ann}(c)$.
- If $\exists i : z_i = 0$ then $g(Z) = 0$.

Lemma 2. Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Denote $f = \sum a_\mathbf{v} X^\mathbf{v}$ and $\operatorname{supp}(f) = \{ \mathbf{v} \in \mathbb{Z}^d \mid a_\mathbf{v} \neq 0 \}$. Define

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

where r is as in Lemma 1 and $\mathbf{v}_0 \in \operatorname{supp}(f)$ arbitrary. Then $g(Z) = 0$ for any common root $Z \in \mathbb{C}^d$ of $\operatorname{Ann}(c)$.

Proof.

- Fix $Z = (z_1, \ldots, z_d) \in \mathbb{C}^d$ a root of $\operatorname{Ann}(c)$.
- If $\exists i : z_i = 0$ then $g(Z) = 0$.
- Assume $\forall i : z_i \neq 0$.

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \mathrm{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- For $\alpha \in \mathbb{C}^*$ define

$$f_\alpha(X) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

LEMMA 2 (2/3)

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \mathrm{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- For $\alpha \in \mathbb{C}^*$ define

$$f_\alpha(X) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

- Plug Z into $f_\alpha(X^{kr+1})$

$$f_\alpha(Z^{kr+1}) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} Z^{(kr+1)\mathbf{v}} = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} \alpha^k Z^{\mathbf{v}} = f_\alpha(Z)\alpha^k$$

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \mathrm{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- For $\alpha \in \mathbb{C}^*$ define

$$f_\alpha(X) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

- Plug Z into $f_\alpha(X^{kr+1})$

$$f_\alpha(Z^{kr+1}) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} Z^{(kr+1)\mathbf{v}} = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} \alpha^k Z^{\mathbf{v}} = f_\alpha(Z)\alpha^k$$

- Z is a root of $f(X^{kr+1})$

$$0 = f(Z^{kr+1}) = f_{\alpha_1}(Z)\alpha_1^k + \cdots + f_{\alpha_n}(Z)\alpha_n^k$$

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \operatorname{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- For $\alpha \in \mathbb{C}^*$ define

$$f_\alpha(X) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \operatorname{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

- Plug Z into $f_\alpha(X^{kr+1})$

$$f_\alpha(Z^{kr+1}) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} Z^{(kr+1)\mathbf{v}} = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} \alpha^k Z^{\mathbf{v}} = f_\alpha(Z)\alpha^k$$

- Z is a root of $f(X^{kr+1})$

$$0 = f(Z^{kr+1}) = f_{\alpha_1}(Z)\alpha_1^k + \cdots + f_{\alpha_n}(Z)\alpha_n^k$$

- Therefore $\forall k \in \mathbb{N}_0$

$$(f_{\alpha_1}(Z), \ldots, f_{\alpha_n}(Z)) \perp (\alpha_1^k, \ldots, \alpha_n^k)$$

Lemma 2 (3/3)

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \mathrm{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$f_\alpha(X) = \sum\nolimits_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- $\forall k \in \mathbb{N}_0 : \; (f_{\alpha_1}(Z), \ldots, f_{\alpha_n}(Z)) \perp (\alpha_1^k, \ldots, \alpha_n^k)$

LEMMA 2 (3/3)

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \mathrm{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$f_\alpha(X) = \textstyle\sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- $\forall k \in \mathbb{N}_0 : \ (f_{\alpha_1}(Z), \ldots, f_{\alpha_n}(Z)) \perp \left(\alpha_1^k, \ldots, \alpha_n^k\right)$
- Vandermonde: $f_\alpha(Z) = 0$

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \mathrm{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$f_\alpha(X) = \textstyle\sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \mathrm{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- $\forall k \in \mathbb{N}_0 : \ (f_{\alpha_1}(Z), \ldots, f_{\alpha_n}(Z)) \perp (\alpha_1^k, \ldots, \alpha_n^k)$
- Vandermonde: $f_\alpha(Z) = 0$
- $\sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} Z^{\mathbf{v}} = 0$

Lemma 2 (3/3)

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \operatorname{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$f_\alpha(X) = \sum\nolimits_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \operatorname{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- $\forall k \in \mathbb{N}_0 \colon \; (f_{\alpha_1}(Z), \ldots, f_{\alpha_n}(Z)) \perp (\alpha_1^k, \ldots, \alpha_n^k)$
- Vandermonde: $f_\alpha(Z) = 0$
- $\sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} Z^{\mathbf{v}} = 0$
- each summand non-zero $\Rightarrow$ at least two summands

$$f = \sum a_{\mathbf{v}} X^{\mathbf{v}} \qquad \operatorname{supp}(f) = \{\, \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \,\} \qquad Z \in (\mathbb{C}^*)^d$$

$$f_\alpha(X) = \sum\nolimits_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}} \qquad S_\alpha = \{\, \mathbf{v} \in \operatorname{supp}(f) \mid Z^{r\mathbf{v}} = \alpha \,\}$$

$$g(X) = x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})$$

- $\forall k \in \mathbb{N}_0 \colon \; (f_{\alpha_1}(Z), \ldots, f_{\alpha_n}(Z)) \perp (\alpha_1^k, \ldots, \alpha_n^k)$
- Vandermonde: $f_\alpha(Z) = 0$
- $\sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} Z^{\mathbf{v}} = 0$
- each summand non-zero $\Rightarrow$ at least two summands
- if $\mathbf{v}_0 \in S_\alpha$ then $\exists \mathbf{v} \in S_\alpha, \mathbf{v} \neq \mathbf{v}_0$ and
$$Z^{r\mathbf{v}} - Z^{r\mathbf{v}_0} = \alpha - \alpha = 0.$$

Definition. Radical of an ideal $A \leq \mathbb{C}[X]$ is

$$\sqrt{A} = \left\{ f \in \mathbb{C}[X] \;\middle|\; \exists m \in \mathbb{N} \colon f^m \in A \right\}$$

Hilbert's Nullstellensatz: f vanishes on all common roots of A if and only if $f \in \sqrt{A}$:

$$\mathbf{I}\mathbf{V}(A) = \sqrt{A}$$

Definition. Radical of an ideal $A \leq \mathbb{C}[X]$ is

$$\sqrt{A} = \left\{ f \in \mathbb{C}[X] \;\middle|\; \exists m \in \mathbb{N} \colon f^m \in A \right\}$$

Hilbert's Nullstellensatz: f vanishes on all common roots of A if and only if $f \in \sqrt{A}$:

$$\mathbf{IV}(A) = \sqrt{A}$$

Lemma 2. Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $f \in \mathbb{Z}[X]$ annihilates c. Choose $\mathbf{v}_0 \in \operatorname{supp}(f)$ arbitrary and let r be as in Lemma 1. Then

$$x_1 \cdots x_d \prod_{\substack{\mathbf{v} \in \operatorname{supp}(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0}) \in \sqrt{\operatorname{Ann}(c)}.$$

Theorem: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $\mathrm{Ann}(c) \neq \{0\}$. Then $\exists \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^d$ such that $(X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1)$ annihilates c.

- There exists $f \in \mathrm{Ann}(c)$, $f \in \mathbb{Z}[X]$

Theorem: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $\mathrm{Ann}(c) \neq \{0\}$. Then $\exists \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^d$ such that $(X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1)$ annihilates c.

- There exists $f \in \mathrm{Ann}(c)$, $f \in \mathbb{Z}[X]$
- Lemma 2 + Nullstellensatz:

$$x_1 \cdots x_d \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0}) \in \sqrt{\mathrm{Ann}(c)}$$

Theorem: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $\mathrm{Ann}(c) \neq \{0\}$. Then $\exists \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^d$ such that $(X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1)$ annihilates c.

- There exists $f \in \mathrm{Ann}(c)$, $f \in \mathbb{Z}[X]$
- Lemma 2 + Nullstellensatz:

$$x_1 \cdots x_d \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0}) \in \sqrt{\mathrm{Ann}(c)}$$

- Exists $m \in \mathbb{N}$: $x_1^m \cdots x_d^m \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})^m \in \mathrm{Ann}(c)$

Theorem: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $\mathrm{Ann}(c) \neq \{0\}$. Then $\exists \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^d$ such that $(X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1)$ annihilates c.

- There exists $f \in \mathrm{Ann}(c)$, $f \in \mathbb{Z}[X]$
- Lemma 2 + Nullstellensatz:

$$x_1 \cdots x_d \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0}) \in \sqrt{\mathrm{Ann}(c)}$$

- Exists $m \in \mathbb{N}$: $x_1^m \cdots x_d^m \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})^m \in \mathrm{Ann}(c)$
- $\prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})^m \in \mathrm{Ann}(c)$

Theorem: Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary and $\mathrm{Ann}(c) \neq \{0\}$. Then $\exists \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^d$ such that $(X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1)$ annihilates c.

- There exists $f \in \mathrm{Ann}(c)$, $f \in \mathbb{Z}[X]$
- Lemma 2 + Nullstellensatz:

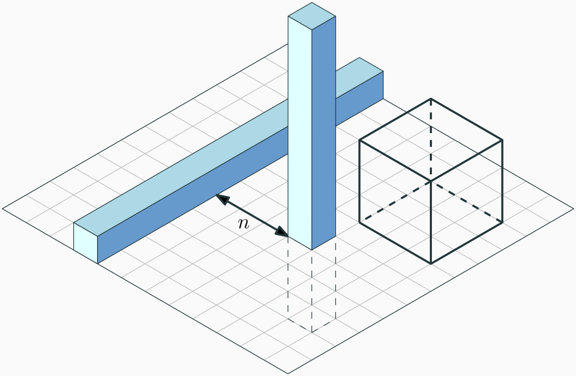
$$x_1 \cdots x_d \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0}) \in \sqrt{\mathrm{Ann}(c)}$$

- Exists $m \in \mathbb{N}$: $x_1^m \cdots x_d^m \prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})^m \in \mathrm{Ann}(c)$
- $\prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r\mathbf{v}} - X^{r\mathbf{v}_0})^m \in \mathrm{Ann}(c)$
- $\prod_{\mathbf{v} \neq \mathbf{v}_0} (X^{r(\mathbf{v} - \mathbf{v}_0)} - 1)^m$ annihilates $\mathrm{Ann}(c)$

Theorem

Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary such that $\mathrm{Ann}(c) \neq 0$. Then there exist periodic $c_1, \ldots, c_n \in \mathbb{Z}[[X^{\pm 1}]]$ such that

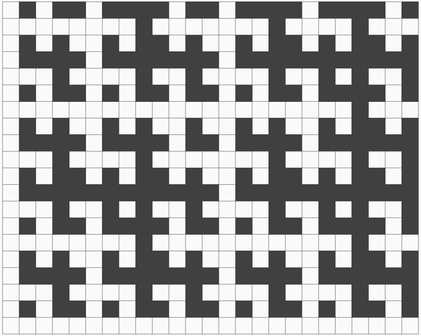
$$c = c_1 + \cdots + c_m.$$



Theorem

Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary such that $\mathrm{Ann}(c) \neq 0$. Then there exist periodic $c_1, \ldots, c_n \in \mathbb{Z}[[X^{\pm 1}]]$ such that

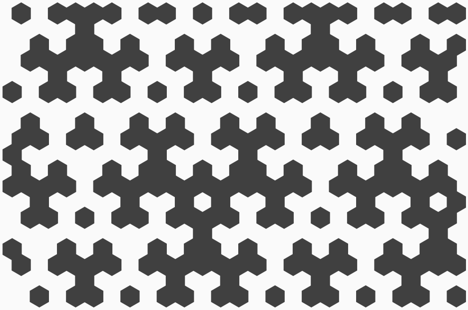
$$c = c_1 + \cdots + c_m.$$



Theorem

Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary such that $\mathrm{Ann}(c) \neq 0$. Then there exist periodic $c_1, \ldots, c_n \in \mathbb{Z}[[X^{\pm 1}]]$ such that

$$c = c_1 + \cdots + c_m.$$



PRIMES AND RADICALS

Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$

Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$
- f^m gives a linear recurring relation on the sequence c

Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$
- f^m gives a linear recurring relation on the sequence c
- c is finitary $\Rightarrow$ c is periodic

Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$
- f^m gives a linear recurring relation on the sequence c
- c is finitary $\Rightarrow$ c is periodic
- $x^p - 1 \in \mathrm{Ann}(c)$

Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$
- f^m gives a linear recurring relation on the sequence c
- c is finitary $\Rightarrow$ c is periodic
- $x^p - 1 \in \mathrm{Ann}(c)$
- $g = \gcd(x^p - 1, f^m) \in \mathrm{Ann}(c)$

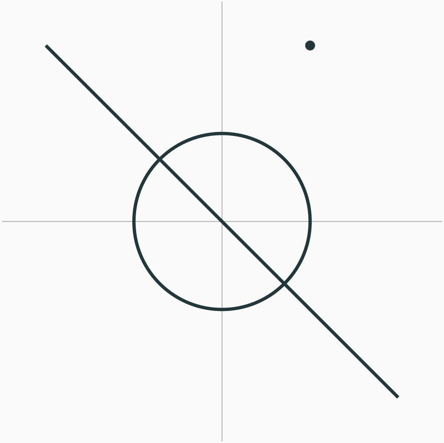
Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$
- f^m gives a linear recurring relation on the sequence c
- c is finitary $\Rightarrow$ c is periodic
- $x^p - 1 \in \mathrm{Ann}(c)$
- $g = \gcd(x^p - 1, f^m) \in \mathrm{Ann}(c)$
- g has only simple roots!

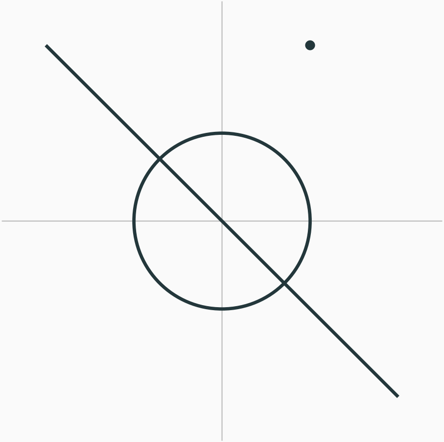
Lemma. Let $c \in \mathbb{C}[x]$ be finitary. Then $\mathrm{Ann}(c)$ is radical.

- Let $f^m \in \mathrm{Ann}(c), f^m \neq 0$
- f^m gives a linear recurring relation on the sequence c
- c is finitary $\Rightarrow$ c is periodic
- $x^p - 1 \in \mathrm{Ann}(c)$
- $g = \gcd(x^p - 1, f^m) \in \mathrm{Ann}(c)$
- g has only simple roots!
- $\Rightarrow g \mid f \Rightarrow f \in \mathrm{Ann}(c)$

PRIME DECOMPOSITION OF RADICALS

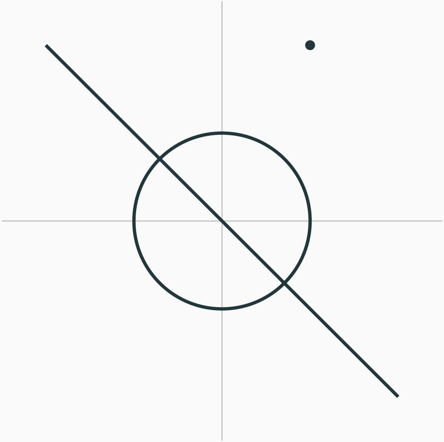


- $\langle x^2 + y^2 - 1 \rangle$
- $\langle x^2 + 2xy + y^2 \rangle$
- $\langle x - 1, y - 2 \rangle$
- $\langle x^2 + y^2 - 1, x + y \rangle$
- $\langle (x^2 + y^2 - 1)(x - 1),$
  $(x^2 + y^2 - 1)(y - 2) \rangle$



- $\langle x^2 + y^2 - 1 \rangle$
- $\langle x^2 + 2xy + y^2 \rangle$
- $\langle x - 1, y - 2 \rangle$
- $\langle x^2 + y^2 - 1, x + y \rangle$
- $\langle (x^2 + y^2 - 1)(x - 1),$
  $(x^2 + y^2 - 1)(y - 2) \rangle$

Theorem. Let $A \leq \mathbb{C}[X]$ be a radical ideal. Then A can be uniquely written as a finite intersection of prime ideals $P_1 \cap \cdots \cap P_k$ such that $P_i \not\subset P_j$ for $i \neq j$.



- $\langle x^2 + y^2 - 1 \rangle$
- $\langle x^2 + 2xy + y^2 \rangle$
- $\langle x - 1, y - 2 \rangle$
- $\langle x^2 + y^2 - 1, x + y \rangle$
- $\langle (x^2 + y^2 - 1)(x - 1),$
  $(x^2 + y^2 - 1)(y - 2) \rangle$

Lemma. Non-zero prime ideals of $\mathbb{C}[x, y]$ are:

- $\langle \varphi \rangle$ for an irreducible polynomial $\phi \in \mathbb{C}[x, y]$
- maximal ideals $\langle x - \alpha, y - \beta \rangle$

Theorem

Let c be a two-dimensional finitary integral configuration. Then Ann(c) is a radical ideal.

Conjecture

Let $c \in \mathbb{Z}[[X^{\pm 1}]]$ be finitary. Then Ann(c) is a radical ideal.

Questions?