On Artin's Conjecture: Pairs of Additive Forms

Miriam Kaesberg

Georg-August Universität Göttingen

April 22, 2021

Artin's Conjecture

Let $f(x_1, \ldots, x_s) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a form (homogeneous polynomial) of degree k. The equation $f(\boldsymbol{x}) = 0$ has a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k^2.$$

Motivation

Artin's Conjecture

Let $f(x_1, \ldots, x_s) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a form (homogeneous polynomial) of degree k. The equation $f(\boldsymbol{x}) = 0$ has a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k^2.$$

Known for:

- $k = 1$,
- $k = 2$ (Meyer),
- $k = 3$ (Lewis).

Motivation

Artin's Conjecture

Let $f(x_1, \ldots, x_s) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a form (homogeneous polynomial) of degree k. The equation $f(\boldsymbol{x}) = 0$ has a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k^2.$$

Known for:

- $k = 1$,
- $k = 2$ (Meyer),
- $k = 3$ (Lewis).

Generalisation

Let $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_s]$ be forms of degree $(k_1, \ldots, k_r)$. The equations $f_1 = \cdots = f_r = 0$ have a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k_1^2 + \cdots + k_r^2.$$

Motivation

Artin's Conjecture

Let $f(x_1, \ldots, x_s) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a form (homogeneous polynomial) of degree k. The equation $f(\boldsymbol{x}) = 0$ has a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k^2.$$

Known for:

- $k = 1$,
- $k = 2$ (Meyer),
- $k = 3$ (Lewis).

Generalisation

Let $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_s]$ be forms of degree $(k_1, \ldots, k_r)$. The equations $f_1 = \cdots = f_r = 0$ have a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k_1^2 + \cdots + k_r^2.$$

True for:

- $k_1 = \cdots = k_r = 1$ (linear algebra),

Artin's Conjecture

Let $f(x_1, \ldots, x_s) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a form (homogeneous polynomial) of degree k. The equation $f(\boldsymbol{x}) = 0$ has a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k^2.$$

Known for:

- $k = 1$,
- $k = 2$ (Meyer),
- $k = 3$ (Lewis).

Generalisation

Let $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_s]$ be forms of degree $(k_1, \ldots, k_r)$. The equations $f_1 = \cdots = f_r = 0$ have a non-trivial solution $\boldsymbol{x} \in \mathbb{Q}_p^s$ for all primes p provided that

$$s > k_1^2 + \cdots + k_r^2.$$

True for:

- $k_1 = \cdots = k_r = 1$ (linear algebra),
- $r = 2$, $k_1 = k_2 = 2$ (Dem'yanov).

How close is Artin's conjecture to the truth?

Counter examples

- 1966: Terjanian: There is a form of degree 4 in 18 variables with no non-trivial 2-adic solution.
- 1966: Browkin: For all p there exist forms without a non-trivial p-adic solution violating Artin's conjecture.
- 1981: Arkhipov and Karatsuba: Not even true if $s > k^n$ for any fixed $n \in \mathbb{N}$.

How close is Artin's conjecture to the truth?

Counter examples

- 1966: Terjanian: There is a form of degree 4 in 18 variables with no non-trivial 2-adic solution.
- 1966: Browkin: For all p there exist forms without a non-trivial p-adic solution violating Artin's conjecture.
- 1981: Arkhipov and Karatsuba: Not even true if $s > k^n$ for any fixed $n \in \mathbb{N}$.

Positive Indications

- Degree: All counter examples are of even degree k.
- Primes: 1965: Ax and Kochen: For a fixed degree k one has a non-trivial p-adic solution for all but finitely many p.
- Forms: 1963: Davenport and Lewis: Artin's conjecture holds for all additive forms.

Counter examples

- 1966: Terjanian: There is a form of degree 4 in 18 variables with no non-trivial 2-adic solution.
- 1966: Browkin: For all p there exist forms without a non-trivial p-adic solution violating Artin's conjecture.
- 1981: Arkhipov and Karatsuba: Not even true if $s > k^n$ for any fixed $n \in \mathbb{N}$.

Positive Indications

- Degree: All counter examples are of even degree k.
- Primes: 1965: Ax and Kochen: For a fixed degree k one has a non-trivial p-adic solution for all but finitely many p.
- Forms: 1963: Davenport and Lewis: Artin's conjecture holds for all additive forms.

Additive Form

A form $f \in \mathbb{Z}[x_1, \ldots, x_s]$ is called additive if $f(x_1, \ldots, x_s) = a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k$.

How close is Artin's conjecture to the truth?

Counter examples

- 1966: Terjanian: There is a form of degree 4 in 18 variables with no non-trivial 2-adic solution.
- 1966: Browkin: For all p there exist forms without a non-trivial p-adic solution violating Artin's conjecture.
- 1981: Arkhipov and Karatsuba: Not even true if $s > k^n$ for any fixed $n \in \mathbb{N}$.

Positive Indications

- Degree: All counter examples are of even degree k.
- Primes: 1965: Ax and Kochen: For a fixed degree k one has a non-trivial p-adic solution for all but finitely many p.
- Forms: 1963: Davenport and Lewis: Artin's conjecture holds for all additive forms.

Additive Form

A form $f \in \mathbb{Z}[x_1, \dots, x_s]$ is called additive if $f(x_1, \dots, x_s) = a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k$.

Generalisation to system of additive forms:

- 1983: Lewis and Montgomery: Not true for all r-tuples $(k_1, k_2, \dots, k_r)$.
- 2015: Wooley: For $r = 2$ there are already counterexamples.

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\mathbf{x}) = g(\mathbf{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\boldsymbol{x}) = g(\boldsymbol{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

- 1969: Davenport, Lewis: Expected bound for odd k holds, $s \geq 7k^3$ holds for even k.

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\mathbf{x}) = g(\mathbf{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

- 1969: Davenport, Lewis: Expected bound for odd k holds, $s \geq 7k^3$ holds for even k.
- 2001: Brüdern, Godinho: Expected bound holds unless

$$k = 2^\tau, \qquad k = 3 \cdot 2^\tau \qquad \text{and} \qquad k = p^\tau (p-1) \qquad (p \geq 3)$$

  for $\tau \geq 1$. Else $s \geq 8k^2$, $s \geq \frac{8}{3}k^2$ and $s \geq 4k^2$ variables, respectively, are sufficient.

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\mathbf{x}) = g(\mathbf{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

- 1969: Davenport, Lewis: Expected bound for odd k holds, $s \geq 7k^3$ holds for even k.
- 2001: Brüdern, Godinho: Expected bound holds unless

$$k = 2^\tau, \qquad k = 3 \cdot 2^\tau \qquad \text{and} \qquad k = p^\tau (p-1) \qquad (p \geq 3)$$

  for $\tau \geq 1$. Else $s \geq 8k^2$, $s \geq \frac{8}{3}k^2$ and $s \geq 4k^2$ variables, respectively, are sufficient.
- 2009: Kränzlein: Expected bound holds for $k = 2^\tau$ for $\tau \geq 16$.

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\mathbf{x}) = g(\mathbf{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

- 1969: Davenport, Lewis: Expected bound for odd k holds, $s \geq 7k^3$ holds for even k.
- 2001: Brüdern, Godinho: Expected bound holds unless

$$k = 2^\tau, \qquad k = 3 \cdot 2^\tau \qquad \text{and} \qquad k = p^\tau (p-1) \qquad (p \geq 3)$$

  for $\tau \geq 1$. Else $s \geq 8k^2$, $s \geq \frac{8}{3}k^2$ and $s \geq 4k^2$ variables, respectively, are sufficient.
- 2009: Kränzlein: Expected bound holds for $k = 2^\tau$ for $\tau \geq 16$.
- 2011, 2013: Godinho, de Souza Neto: For $k = p^\tau (p-1)$ it is sufficient if $s > 2\frac{p}{p-1}k^2 - 2k$ holds and either $p \in \{3, 5\}$ or $p \geq 7$ and $\tau \geq \frac{p-1}{2}$

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\mathbf{x}) = g(\mathbf{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

- 1969: Davenport, Lewis: Expected bound for odd k holds, $s \geq 7k^3$ holds for even k.
- 2001: Brüdern, Godinho: Expected bound holds unless

$$k = 2^\tau, \qquad k = 3 \cdot 2^\tau \qquad \text{and} \qquad k = p^\tau (p-1) \qquad (p \geq 3)$$

  for $\tau \geq 1$. Else $s \geq 8k^2$, $s \geq \frac{8}{3}k^2$ and $s \geq 4k^2$ variables, respectively, are sufficient.
- 2009: Kränzlein: Expected bound holds for $k = 2^\tau$ for $\tau \geq 16$.
- 2011, 2013: Godinho, de Souza Neto: For $k = p^\tau (p-1)$ it is sufficient if $s > 2\frac{p}{p-1}k^2 - 2k$ holds and either $p \in \{3, 5\}$ or $p \geq 7$ and $\tau \geq \frac{p-1}{2}$
- 2013: Godinho, Knapp and Rodrigues: Expected bound holds for $k = 6$.

$r = 2$ and $k_1 = k_2$

Let f, g be two additive forms with integer coefficients in s variables of degree k.

Question

How big does s have to be to ensure a non-trivial p-adic solution $f(\mathbf{x}) = g(\mathbf{x}) = 0$ for all primes p?

Expected Bound: $s \geq 2k^2 + 1$ suffices

- 1969: Davenport, Lewis: Expected bound for odd k holds, $s \geq 7k^3$ holds for even k.
- 2001: Brüdern, Godinho: Expected bound holds unless

$$k = 2^\tau, \qquad k = 3 \cdot 2^\tau \qquad \text{and} \qquad k = p^\tau(p-1) \qquad (p \geq 3)$$

  for $\tau \geq 1$. Else $s \geq 8k^2$, $s \geq \frac{8}{3}k^2$ and $s \geq 4k^2$ variables, respectively, are sufficient.
- 2009: Kränzlein: Expected bound holds for $k = 2^\tau$ for $\tau \geq 16$.
- 2011, 2013: Godinho, de Souza Neto: For $k = p^\tau(p-1)$ it is sufficient if $s > 2\frac{p}{p-1}k^2 - 2k$ holds and either $p \in \{3, 5\}$ or $p \geq 7$ and $\tau \geq \frac{p-1}{2}$
- 2013: Godinho, Knapp and Rodrigues: Expected bound holds for $k = 6$.
- 2017: Godinho, Ventura: Expected bound hold for $k = 3^\tau \cdot 2$.

Result

Theorem (K.)

For $p \geq 5$ prime, $\tau \geq 1$ and $k = p^\tau (p-1)$ the pair of additive forms with integers coefficients

$$\sum_{j=1}^{s} a_j x_j^k = \sum_{j=1}^{s} b_j x_j^k = 0$$

have a non-trivial p-adic solution if $s \geq 2k^2 + 1$.

Theorem (K.)

For $p \geq 5$ prime, $\tau \geq 1$ and $k = p^{\tau}(p-1)$ the pair of additive forms with integers coefficients

$$\sum_{j=1}^{s} a_j x_j^k = \sum_{j=1}^{s} b_j x_j^k = 0$$

have a non-trivial p-adic solution if $s \geq 2k^2 + 1$.

Missing values of k:

- 2^{τ} with $2 \leq \tau \leq 15$
- $3 \cdot 2^{\tau}$ with $2 \leq \tau (\leq 15)$

Finding p-adic solutions

Let $f(x_1, \ldots, x_s) = \sum_{i=1}^{s} a_i x_i^k$ and $g(x_1, \ldots, x_s) = \sum_{i=1}^{s} b_i x_i^k$.
For $k = p^\tau k_0$ with $\gcd(p, k_0) = 1$ define

$$\gamma := \begin{cases} 1, & \text{if } \tau = 0 \\ \tau + 1, & \text{if } \tau > 0 \text{ and } p > 2 \\ \tau + 2, & \text{if } \tau > 0 \text{ and } p = 2. \end{cases}$$

Finding p-adic solutions

Let $f(x_1,\ldots,x_s)=\sum_{i=1}^s a_i x_i^k$ and $g(x_1,\ldots,x_s)=\sum_{i=1}^s b_i x_i^k$.
For $k=p^\tau k_0$ with $\gcd(p,k_0)=1$ define

$$\gamma := \begin{cases} 1, & \text{if } \tau = 0 \\ \tau+1, & \text{if } \tau > 0 \text{ and } p > 2 \\ \tau+2, & \text{if } \tau > 0 \text{ and } p = 2. \end{cases}$$

Hensel's Lemma

If the congruences

$$\sum_{i=1}^s a_i x_i^k \equiv 0 \mod p^\gamma, \qquad \sum_{i=1}^s b_i x_i^k \equiv 0 \mod p^\gamma$$

have a solution in the integers for which the matrix

$$\begin{pmatrix} a_1x_1 & a_2x_2 & \ldots & a_sx_s \\ b_1x_1 & b_2x_2 & \ldots & b_sx_s \end{pmatrix}$$

has rank 2 modulo p, then the pair of forms f,g has a non-trivial p-adic solution.

p-normalized Pairs

Equivalence relation defined via the operations:

- $f' = f\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right), \; g' = g\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right)$ for integers ν_i
- $f'' = \lambda_1 f + \lambda_2 g, \; g'' = \mu_1 f + \mu_2 g$ for $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Q}$ with $\lambda_1\mu_2 - \lambda_2\mu_1 \neq 0$.

p-normalized Pairs

Equivalence relation defined via the operations:

- $f' = f\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right), \; g' = g\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right)$ for integers ν_i
- $f'' = \lambda_1 f + \lambda_2 g, \; g'' = \mu_1 f + \mu_2 g$ for $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Q}$ with $\lambda_1\mu_2 - \lambda_2\mu_1 \neq 0$.

p-equivalence classes

A pair $(\tilde{f}, \tilde{g})$ lies in the same p-equivalence class as (f, g) if it can be obtained by a finite succession of the above operations.

p-normalized Pairs

Equivalence relation defined via the operations:

- $f' = f\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right),\ g' = g\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right)$ for integers ν_i
- $f'' = \lambda_1 f + \lambda_2 g,\ g'' = \mu_1 f + \mu_2 g$ for $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Q}$ with $\lambda_1\mu_2 - \lambda_2\mu_1 \neq 0$.

p-equivalence classes

A pair $(\tilde{f}, \tilde{g})$ lies in the same p-equivalence class as (f, g) if it can be obtained by a finite succession of the above operations.

$$\vartheta(f, g) := \prod_{\substack{1\le i,j\le s \\ i\neq j}} \left(a_i b_j - a_j b_i\right)$$

p-normalized Pairs

Equivalence relation defined via the operations:

- $f' = f\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right), \; g' = g\left(p^{\nu_1}x_1, \ldots, p^{\nu_s}x_s\right)$ for integers ν_i
- $f'' = \lambda_1 f + \lambda_2 g, \; g'' = \mu_1 f + \mu_2 g$ for $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Q}$ with $\lambda_1\mu_2 - \lambda_2\mu_1 \neq 0$.

p-equivalence classes

A pair $(\tilde{f}, \tilde{g})$ lies in the same p-equivalence class as (f, g) if it can be obtained by a finite succession of the above operations.

$$\vartheta(f, g) := \prod_{\substack{1 \leq i,j \leq s \\ i \neq j}} \left(a_i b_j - a_j b_i\right)$$

Definition

A p-normalised pair f, g is a pair of forms with integers coefficients and $\vartheta(f, g) \neq 0$, where the power of p dividing $\vartheta(f, g)$ is as small as possible among all pairs of forms in the same p-equivalent class.

Some Notation

Definition

A variable x_i is called **at level** l if $\begin{pmatrix} a_i \\ b_i \end{pmatrix} = p^l \begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix}$ and $p \nmid \begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix}$. The vector $\begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix}$ is called the **level coefficient vector** of x_i.

Definition

A variable x_i is called **at level** l if $\begin{pmatrix} a_i \\ b_i \end{pmatrix} = p^l \begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix}$ and $p \nmid \begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix}$. The vector $\begin{pmatrix} \tilde{a}_i \\ \tilde{b}_i \end{pmatrix}$ is called the **level coefficient vector** of x_i.

Definition

Define

$$\mathscr{L}_0 := \left\{ c \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid 1 \leq c \leq p-1 \right\} \quad \text{and} \quad \mathscr{L}_\nu := \left\{ c \begin{pmatrix} \nu \\ 1 \end{pmatrix} \mid 1 \leq c \leq p-1 \right\}$$

for all $1 \leq \nu \leq p$. One says that the variable x_i **is of colour** ν, if $\binom{\tilde{a}_i}{\tilde{b}_i} \in \mathscr{L}_\nu \mod p$.

Properties of p-normalised pairs

- There are no variables at level k or higher.

Properties of p-normalised pairs

- There are no variables at level k or higher.

$$
\begin{aligned}
f &= f_0 + pf_1 + \cdots + p^{k-1} f_{k-1}, \qquad & f_i &= \sum_{x_j \text{ at level } i} \tilde{a}_j x_j^k \\
g &= g_0 + pg_1 + \cdots + p^{k-1} g_{k-1}, \qquad & g_i &= \sum_{x_j \text{ at level } i} \tilde{b}_j x_j^k
\end{aligned}
$$

Properties of p-normalised pairs

- There are no variables at level k or higher.

$$f = f_0 + pf_1 + \cdots + p^{k-1} f_{k-1}, \qquad f_i = \sum_{x_j \text{ at level } i} \tilde{a}_j x_j^k$$

$$g = g_0 + pg_1 + \cdots + p^{k-1} g_{k-1}, \qquad g_i = \sum_{x_j \text{ at level } i} \tilde{b}_j x_j^k$$

- Let there be m_i variables at level i.

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

- There are no variables at level k or higher.

$$f = f_0 + pf_1 + \cdots + p^{k-1} f_{k-1}, \qquad f_i = \sum_{x_j \text{ at level } i} \tilde{a}_j x_j^k$$

$$g = g_0 + pg_1 + \cdots + p^{k-1} g_{k-1}, \qquad g_i = \sum_{x_j \text{ at level } i} \tilde{b}_j x_j^k$$

- Let there be m_i variables at level i.

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

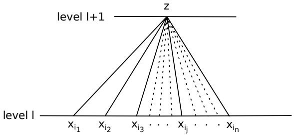
- Let q_i be the number of variables at level i which are not in the biggest colour.

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j + \frac{1}{2}\right) s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

Contraction

Goal:

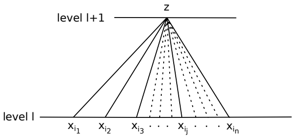
$$\sum_{i=1}^{s} a_i x_i^k \equiv 0 \mod p^\gamma, \qquad \sum_{i=1}^{s} b_i x_i^k \equiv 0 \mod p^\gamma \qquad \text{(solve)}$$



$$\begin{pmatrix} a_1x_1 & a_2x_2 & \dots & a_sx_s \\ b_1x_1 & b_2x_2 & \dots & b_sx_s \end{pmatrix} \qquad \text{(rank 2 modulo } p\text{)}$$

Goal:

$$\sum_{i=1}^{s} a_i x_i^k \equiv 0 \mod p^\gamma, \qquad \sum_{i=1}^{s} b_i x_i^k \equiv 0 \mod p^\gamma \qquad \text{(solve)}$$



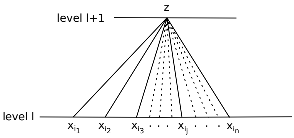
$$\begin{pmatrix} a_1x_1 & a_2x_2 & \dots & a_sx_s \\ b_1x_1 & b_2x_2 & \dots & b_sx_s \end{pmatrix} \qquad \text{(rank 2 modulo } p\text{)}$$

- Setting a variable at level at least γ to 1 and all other 0 solves the equation.

Contraction

Goal:

$$\sum_{i=1}^{s} a_i x_i^k \equiv 0 \mod p^\gamma, \qquad \sum_{i=1}^{s} b_i x_i^k \equiv 0 \mod p^\gamma \qquad \text{(solve)}$$



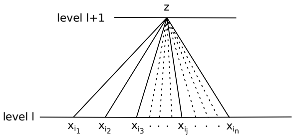
$$\begin{pmatrix} a_1 x_1 & a_2 x_2 & \dots & a_s x_s \\ b_1 x_1 & b_2 x_2 & \dots & b_s x_s \end{pmatrix} \qquad \text{(rank 2 modulo } p\text{)}$$

- Setting a variable at level at least γ to 1 and all other 0 solves the equation.
- Setting two variables at different colour at level 0 to a value not divisible by p takes care of the rank condition.

Contraction

Goal:

$$\sum_{i=1}^{s} a_i x_i^k \equiv 0 \mod p^\gamma, \qquad \sum_{i=1}^{s} b_i x_i^k \equiv 0 \mod p^\gamma \qquad \text{(solve)}$$



$$\begin{pmatrix} a_1x_1 & a_2x_2 & \dots & a_sx_s \\ b_1x_1 & b_2x_2 & \dots & b_sx_s \end{pmatrix} \qquad \text{(rank 2 modulo } p\text{)}$$

- Setting a variable at level at least γ to 1 and all other 0 solves the equation.
- Setting two variables at different colour at level 0 to a value not divisible by p takes care of the rank condition.

Definition

Let $x_{i_1}, \dots, x_{i_n}$ variables at level l and $y_1, \dots, y_n \in \mathbb{Z} \setminus p\mathbb{Z}$ such that

$$\sum_{j=1}^{n} a_{i_j} y_j^k \equiv \sum_{j=1}^{n} b_{i_j} y_j^k \equiv 0 \mod p^{l+1},$$

then the variables x_{i_j} **contract** to a variable at level at least $l+1$.

Procedure

Primary variables

A variable which can be "traced back" to two different colours at level 0 is called primary.

Procedure

Primary variables

A variable which can be "traced back" to two different colours at level 0 is called primary.

Goal: Create a primary variable at level at least γ.

Primary variables

A variable which can be "traced back" to two different colours at level 0 is called primary.

Goal: Create a primary variable at level at least γ.

- Use the variables at level 0 to create primary variables:
  Davenport and Lewis: One can contract at least $\min\left(\left\lfloor \frac{m_0}{2p-1} \right\rfloor, \left\lfloor \frac{q_0}{p} \right\rfloor\right)$ primary variables at level at least 1.

Primary variables

A variable which can be "traced back" to two different colours at level 0 is called primary.

Goal: Create a primary variable at level at least γ.

- Use the variables at level 0 to create primary variables:
  Davenport and Lewis: One can contract at least $\min\left(\left\lfloor \frac{m_0}{2p-1} \right\rfloor, \left\lfloor \frac{q_0}{p} \right\rfloor\right)$ primary variables at level at least 1.
- Lift the primary variables to higher levels.

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1$

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1 \Rightarrow \sum_{i=1}^{2p-1} \binom{\tilde{a}_i}{\tilde{b}_i} x_i^k \equiv 0 \mod p$

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1 \Rightarrow \sum_{i=1}^{2p-1} \binom{\tilde{a}_i}{\tilde{b}_i} x_i^k \equiv 0 \mod p$

Lemma (Olson)

A set of $3p-2$ variables at level at least l contains a contraction of at most p variables to a variable at level at least $l+1$.

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1 \Rightarrow \sum_{i=1}^{2p-1} \binom{\tilde{a}_i}{\tilde{b}_i} x_i^k \equiv 0 \mod p$$

Lemma (Olson)

A set of $3p-2$ variables at level at least l contains a contraction of at most p variables to a variable at level at least $l+1$.

$$D\left((\mathbb{Z}/p\mathbb{Z})^3\right) = 3p-2 \Rightarrow \text{It exists } \emptyset \neq J \subset \{1,\ldots,3p-2\}, \text{ s. t. } \sum_{j\in J} \begin{pmatrix} \tilde{a}_j \\ \tilde{b}_j \\ 1 \end{pmatrix} \equiv 0 \mod p.$$

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1 \Rightarrow \sum_{i=1}^{2p-1} \binom{\tilde{a}_i}{\tilde{b}_i} x_i^k \equiv 0 \mod p$

Lemma (Olson)

A set of $3p-2$ variables at level at least l contains a contraction of at most p variables to a variable at level at least $l+1$.

$D\left((\mathbb{Z}/p\mathbb{Z})^3\right) = 3p-2 \Rightarrow$ It exists $\emptyset \neq J \subset \{1,\ldots,3p-2\}$, s. t. $\sum_{j\in J} \begin{pmatrix} \tilde{a}_j \\ \tilde{b}_j \\ 1 \end{pmatrix} \equiv 0 \mod p$.

If $|J| = 2p$ it exists a contraction $\tilde{J} \subset J$ with $|\tilde{J}| \leq 2p-1$.

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1 \Rightarrow \sum_{i=1}^{2p-1} \binom{\tilde{a}_i}{\tilde{b}_i} x_i^k \equiv 0 \mod p$$

Lemma (Olson)

A set of $3p-2$ variables at level at least l contains a contraction of at most p variables to a variable at level at least $l+1$.

$$D\left((\mathbb{Z}/p\mathbb{Z})^3\right) = 3p-2 \Rightarrow \text{It exists } \emptyset \neq J \subset \{1,\ldots,3p-2\}, \text{ s. t. } \sum_{j\in J} \begin{pmatrix} \tilde{a}_j \\ \tilde{b}_j \\ 1 \end{pmatrix} \equiv 0 \mod p.$$

If $|J| = 2p$ it exists a contraction $\tilde{J} \subset J$ with $|\tilde{J}| \leq 2p-1$.

$\rightarrow$ Lifting primary variables one level higher, one loses about a factor p.

Lifting primary variables

Lemma (Olson)

A set of $2p-1$ variables at level at least l contains a contraction to a variable at level at least $l+1$.

$$D\left((\mathbb{Z}/p\mathbb{Z})^2\right) = 2p-1 \Rightarrow \sum_{i=1}^{2p-1} \binom{\tilde{a}_i}{\tilde{b}_i} x_i^k \equiv 0 \mod p$$

Lemma (Olson)

A set of $3p-2$ variables at level at least l contains a contraction of at most p variables to a variable at level at least $l+1$.

$$D\left((\mathbb{Z}/p\mathbb{Z})^3\right) = 3p-2 \Rightarrow \text{It exists } \emptyset \neq J \subset \{1,\ldots,3p-2\}, \text{ s. t. } \sum_{j\in J} \begin{pmatrix} \tilde{a}_j \\ \tilde{b}_j \\ 1 \end{pmatrix} \equiv 0 \mod p.$$

If $|J| = 2p$ it exists a contraction $\tilde{J} \subset J$ with $|\tilde{J}| \leq 2p-1$.

→ Lifting primary variables one level higher, one loses about a factor p.
→ Gives at best the bound $s > 2\frac{p}{p-1}k^2 - 2k$.

Reducing the lost factor

Lemma

A set of $2p-2$ variables at level l ($p-1$ of some colour ν and $p-1$ not of colour ν) contract together with a primary variable at level at least l to a primary variable at level at least $l+1$.

Reducing the lost factor

Lemma

A set of $2p-2$ variables at level l ($p-1$ of some colour ν and $p-1$ not of colour ν) contract together with a primary variable at level at least l to a primary variable at level at least $l+1$.

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j+\frac{1}{2}\right)s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

Reducing the lost factor

Lemma

A set of $2p-2$ variables at level l ($p-1$ of some colour ν and $p-1$ not of colour ν) contract together with a primary variable at level at least l to a primary variable at level at least $l+1$.

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{(j+\frac{1}{2})\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

Extreme cases:

Big m_0 and q_0.

At least $m_i \geq 2p-1$ and $q_i \geq p$ for all i.

Reducing the lost factor

Lemma

A set of $2p-2$ variables at level l ($p-1$ of some colour ν and $p-1$ not of colour ν) contract together with a primary variable at level at least l to a primary variable at level at least $l+1$.

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j+\frac{1}{2}\right)s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

Extreme cases:

Big m_0 and q_0.

Big m_0 but only small q_0.

At least $m_i \geq 2p-1$ and $q_i \geq p$ for all i.

Reducing the lost factor

Lemma

A set of $2p-2$ variables at level l ($p-1$ of some colour ν and $p-1$ not of colour ν) contract together with a primary variable at level at least l to a primary variable at level at least $l+1$.

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j+\frac{1}{2}\right)s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

Extreme cases:

Big m_0 and q_0.
Big m_0 but only small q_0.

At least $m_i \geq 2p-1$ and $q_i \geq p$ for all i.

$\rightarrow$ Take unused variables at lower levels to create helpful variables along the way.

Level and colour control

Define

$$\mathscr{L}_{0\mu} := \left\{ c\left(\begin{pmatrix}1\\0\end{pmatrix} + \mu\begin{pmatrix}0\\p\end{pmatrix}\right) \mid c \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^* \right\}$$
$$\mathscr{L}_{\nu\mu} := \left\{ c\left(\begin{pmatrix}\nu\\1\end{pmatrix} + \mu\begin{pmatrix}p\\0\end{pmatrix}\right) \mid c \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^* \right\}$$

for all $0 \leq \nu \leq p$ and $0 \leq \mu \leq p-1$. One says that the variable x_i is of colour nuance (ν, μ), if $\begin{pmatrix}\tilde{a}_i\\\tilde{b}_i\end{pmatrix} \in \mathscr{L}_{\nu\mu} \mod p^2$.

Level and colour control

Define

$$\mathscr{L}_{0\mu} := \left\{ c\left(\begin{pmatrix}1\\0\end{pmatrix} + \mu\begin{pmatrix}0\\p\end{pmatrix}\right) \mid c \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^* \right\}$$
$$\mathscr{L}_{\nu\mu} := \left\{ c\left(\begin{pmatrix}\nu\\1\end{pmatrix} + \mu\begin{pmatrix}p\\0\end{pmatrix}\right) \mid c \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^* \right\}$$

for all $0 \leq \nu \leq p$ and $0 \leq \mu \leq p-1$. One says that the variable x_i is of colour nuance (ν, μ), if $\begin{pmatrix}\tilde{a}_i\\\tilde{b}_i\end{pmatrix} \in \mathscr{L}_{\nu\mu} \mod p^2$.

Lemma

A set of $3p-2$ variables at level l and colour nuance (ν, μ) contains a contraction of at most p variables to a variable a level $l+1$ and colour ν.

An alternative to primary variables

Creating primary variables is expensive: $2p - 1$ variables at level 0, from which p are not in the biggest colour.

An alternative to primary variables

Creating primary variables is expensive: $2p - 1$ variables at level 0, from which p are not in the biggest colour.

Alternative way if $m_0 - q_0$ is big:

- The variables at level 0 not in the biggest colour take the place of primary variables.

An alternative to primary variables

Creating primary variables is expensive: $2p - 1$ variables at level 0, from which p are not in the biggest colour.

Alternative way if $m_0 - q_0$ is big:

- The variables at level 0 not in the biggest colour take the place of primary variables.
  $\rightarrow$ Goal: Create a variable at level γ which traces back to one of those.

An alternative to primary variables

Creating primary variables is expensive: $2p - 1$ variables at level 0, from which p are not in the biggest colour.

Alternative way if $m_0 - q_0$ is big:

- The variables at level 0 not in the biggest colour take the place of primary variables.
  $\rightarrow$ Goal: Create a variable at level γ which traces back to one of those.
- Use the (many) variables at level 0 in the biggest colour to create helpful variables.

Level rotation

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j+\frac{1}{2}\right)s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

Level rotation

$$m_0 + \cdots + m_j \geq \frac{(j+1)\, s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j + \frac{1}{2}\right) s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$f = f_0 + p f_1 + p^2 f_2 + \cdots + p^{k-1} f_{k-1}$$

$$g = g_0 + p g_1 + p^2 g_2 + \cdots + p^{k-1} g_{k-1}$$

Level rotation

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$
$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{(j+\frac{1}{2})\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$f = f_0 + pf_1 + p^2 f_2 + \cdots + p^{k-1} f_{k-1}$$
$$g = g_0 + pg_1 + p^2 g_2 + \cdots + p^{k-1} g_{k-1}$$

$$\Downarrow$$

$$f = p^k f_0 + pf_1 + p^2 f_2 + \cdots + p^{k-1} f_{k-1}$$
$$g = p^k g_0 + pg_1 + p^2 g_2 + \cdots + p^{k-1} g_{k-1}$$

Level rotation

$$m_0 + \cdots + m_j \geq \frac{(j+1)\,s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$m_0 + \cdots + m_{j-1} + q_j \geq \frac{\left(j+\frac{1}{2}\right)s}{k} \qquad \text{for} \qquad j = 0, 1, \ldots, k-1$$

$$f = f_0 + pf_1 + p^2 f_2 + \cdots + p^{k-1} f_{k-1}$$

$$g = g_0 + pg_1 + p^2 g_2 + \cdots + p^{k-1} g_{k-1}$$

$$\Downarrow$$

$$f = p^k f_0 + pf_1 + p^2 f_2 + \cdots + p^{k-1} f_{k-1}$$

$$g = p^k g_0 + pg_1 + p^2 g_2 + \cdots + p^{k-1} g_{k-1}$$

$$\Downarrow$$

$$f = p^{k-1} f_0 + f_1 + pf_2 + \cdots + p^{k-2} f_{k-1}$$

$$g = p^{k-1} g_0 + g_1 + pg_2 + \cdots + p^{k-2} g_{k-1}$$

Summary

- Produce primary variables (or work with the altenative, if $m_0 - q_0$ is big enough).
- Lift them to higher level, trying to minimise the factor which is lost with each lifting.
- Either reach at least level γ or gather information about the distribution of the variables at low levels.
- If necessary use level rotation to expand the knowledge to higher levels.

Thanks for your attention!