Arora-GB: Algebraic Algorithms for LWE Problems

Martin R. Albrecht[2]

Information Security Group, Royal Holloway, University of London

ENS Lyon, 9. October 2014

[2] joint work with L. Perret, C. Cid, J.-C. Faugère and R. Fitzpatrick

Contents

Learning with Errors

Definition (LWE)

Let $n \geq 1$ be an integer, q be an odd integer, χ be a probability distribution on $\mathbb{Z}_q$ and $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector. We denote by $L_{\mathbf{s},\chi}^{(n)}$ the probability distribution on $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$ obtained by choosing $G \in \mathbb{Z}_q^{n\times m}$ uniformly at random, sampling $\mathbf{e}$ according to $\chi_{\alpha,q}^m$, and returning

$$(G, \mathbf{s} \times G + \mathbf{e}) = (G, \mathbf{c}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m.$$

LWE is the problem of finding $\mathbf{s} \in \mathbb{Z}_q^n$ from $(G, \mathbf{s} \times G + \mathbf{e})$ sampled according to $L_{\mathbf{s},\chi}^{(n)}$.

Noise Distribution

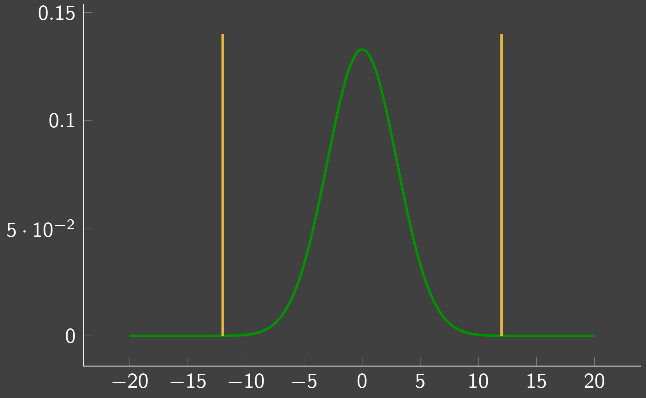
- $\chi_{\alpha,q}$ is a discrete Gaussian distribution over $\mathbb{Z}$ with standard deviation
$$\sigma = \frac{\alpha\, q}{\sqrt{2\pi}}$$
considered modulo q.
- A typical setting for the standard deviation is $\sigma = n^{\epsilon}$, with $0 \leq \epsilon \leq 1$.
- As soon as $\epsilon > 1/2$, (worst-case) $\mathrm{GAPSVP} - \tilde{\mathcal{O}}(n/\alpha)$ classically reduces to (average-case) LWE

Any algorithm solving LWE (when $\epsilon > 1/2$) can be used to solve $\mathrm{GAPSVP} - \tilde{\mathcal{O}}(n/\alpha)$.

Arora-Ge Idea I

The noise follows a discrete Gaussian distribution, we have:

$$\Pr[e \leftarrow_{\$} \chi : |e| > C \cdot \sigma] \leq \frac{2}{C\sqrt{2\pi}} e^{-C^2/2} \in e^{\mathcal{O}(-C^2)}.$$



Arora-Ge Idea II

If $e \leftarrow_{\$} \chi$ and

$$P(X) = X \prod_{i=1}^{C\cdot\sigma}(X+i)(X-i),$$

we have $P(e) = 0$ with probability at least $1 - e^{\mathcal{O}(-C^2)}$.

So if $(\mathbf{a}, c) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, and $e \leftarrow_{\$} \chi$, then

$$P\big(-c + \sum_{j=1}^{n} \mathbf{a}_{(j)} x_j\big) = 0, \tag{1}$$

with probability at least $1 - e^{\mathcal{O}(-C^2)}$.

Arora-Ge Idea III

Each $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) = (\mathbf{a}, c)$ generates a **non-linear equation** of degree $2C\sigma + 1$ in the n components of the secret $\mathbf{s}$ which holds with probability $1 - e^{\mathcal{O}(-C^2)}$.

Arora-Ge Idea

Solve this non-linear system of equations to solve LWE.

From Arora-Ge to Arora-GB

Arora & Ge solve the non-linear system using linearisation which requires $O(n^d)$ samples to solve equations at degree d.

However, this might not be optimal, as more samples

1. increase the **number of equations** $\rightarrow$ solving is **easier**.
2. increase the required interval $C\sigma$ and hence the **degree** $\rightarrow$ solving is **harder**.

Our idea

Solve this non-linear system of equations using Gröbner bases.

BinaryError-LWE

Theorem (BinaryError-LWE)

Let $n, m = n\left(1 + \Omega\big(1/\log(n)\big)\right)$ be integers, and $q \geq n^{\mathcal{O}(1)}$ be a sufficiently large polynomially bounded (prime) modulus.

Then, solving LWE with parameters n, m, q and independent uniformly random binary errors is at least as hard as approximating lattice problems in the worst-case on $\Theta\big(n/\log(n)\big)$–dimensional lattices within a factor $\tilde{\mathcal{O}}(\sqrt{n} \cdot q)$.

From Arora-Ge we know that this problem is easy if $m = \mathcal{O}\left(n^2\right)$. But what about

$$n\left(1 + \Omega\big(1/\log(n)\big)\right) < m < \mathcal{O}\left(n^2\right)?$$

Fröberg's Conjecture

- All our results depend on assumptions that the generated systems are **semi-regular**.
- These assumptions are related to Fröberg's conjecture in algebraic geometry.
- We cannot prove our assumptions or his conjecture but we report on some progress in that direction.

Contents

Arora & Ge Complexity

- The analysis of the Arora-Ge algorithm hides constants **in the exponent** and logarithm factors.
- Th overall complexity is that of Gaussian elimination on a matrix of size

$$M_{\mathrm{AG}} \times \binom{n + D_{\mathrm{AG}}}{D_{\mathrm{AG}}}.$$

- Gaussian elimination on an $m \times n$ matrix of rank r has complexity

$$\mathcal{O}\left(mnr^{\omega-2}\right).$$

Arora & Ge Complexity

$$\mathcal{O}\left(M_{\mathrm{AG}} \cdot \binom{n + D_{\mathrm{AG}}}{D_{\mathrm{AG}}}^{\omega-1}\right) = \mathcal{O}\left(M_{\mathrm{AG}} \cdot \binom{n + 2\,C_{\mathrm{AG}}\,\sigma + 1}{2\,C_{\mathrm{AG}}\,\sigma + 1}^{\omega-1}\right).$$

Bounding C_{AG} I

Lemma

Let $n, q, \sigma = \alpha \cdot q$ *be parameters of an* $\mathrm{LWE}_{\chi_{\alpha,q}}$ *instance where* $q = \mathrm{poly}(n)$. *Let* $p'_f \in [0,1]$ *be a constant upper bound on the probability of failure and*

$$C_{\mathrm{AG}} \leq 2\,\sigma \log n + a^{1/2} \approx 4\,\sigma \log n,$$

with

$$a = 4(\sigma \log n)^2 + 2\log(\sigma\, q \log q) - 2\log p'_f + 2\log n.$$

Finally, let also $D_{\mathrm{AG}} = 2\,C_{\mathrm{AG}}\,\sigma + 1$. *Then, the system obtained by linearizing*

$$\binom{n + D_{\mathrm{AG}}}{D_{\mathrm{AG}}} \sigma\, q \log q$$

equations of degree as in (1) *is such that the secret is a zero of all the polynomials, with probability bigger than* $1 - p'_f$.

Bounding C_{AG} II

Proof.

1. The probability of failure is upper bounded by:

$$\begin{aligned} p_f &= M_{\mathrm{AG}} \times \Pr[e \xleftarrow{\$} \chi_{\alpha,q} : |e| > C_{\mathrm{AG}} \cdot \sigma] \\ &< \frac{\binom{n+D_{\mathrm{AG}}}{D_{\mathrm{AG}}} \sigma\, q \log q}{C_{\mathrm{AG}} \cdot e^{C_{\mathrm{AG}}^2/2}} = p_f'. \end{aligned}$$

2. Bound $\binom{n+D_{\mathrm{AG}}}{D_{\mathrm{AG}}}$ by $n^{D_{\mathrm{AG}}}$ and solve for C_{AG}. We get

$$C_{\mathrm{AG}} = 2\,\sigma \cdot \log(n) + a^{1/2},$$

   with $a = 4(\sigma \log n)^2 + 2\log(\sigma\, q \log q) - 2\log p_f' + 2\log n$.

3. For $q \in \mathrm{poly(n)}$, p_f' a constant and n big enough:

$$a \approx 4(\sigma \log n)^2.$$

Result

Theorem

Let $n, q, \sigma = \alpha \cdot q$ be parameters of an $\mathrm{LWE}_{\chi_{\alpha,q}}$ instance. If $n \in o(\sigma^2 \log(n))$ then the Arora & Ge algorithm solves the computational LWE problem in time complexity

$$\mathcal{O}\left(2^{\,\omega \cdot n \log \frac{D_{\mathrm{AG}}}{n}} \cdot \sigma\, q \log q\right) =$$

$$\mathcal{O}\left(2^{\,\omega\, n \log(8\,\sigma^2 \log n) - n \log n} \cdot \mathrm{poly}(n)\right)$$

Contents

Gröbner Bases I

Definition (Gröbner Basis)

Let $\mathcal{I}$ be an ideal of $\mathbb{Z}_q[x_1, \ldots, x_n]$ and fix a monomial ordering. A finite subset

$$G = \{g_1, \ldots, g_m\} \subset \mathcal{I}$$

is said to be a **Gröbner basis** of $\mathcal{I}$ if

$$\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m) \rangle = \langle \mathrm{LM}(\mathcal{I}) \rangle.$$

If a system of equations has one common root, the Gröbner basis of the ideal spanned by its polynomials is $[x_1 - s_1, \ldots, x_n - s_n]$ where $\mathbf{s} = (s_1, \ldots, s_n)$ is the common root.

Gröbner Bases II

Theorem

Let q be a prime and let $\mathbf{f} = (f_1, \ldots, f_m) \in (\mathbb{Z}_q[x_1, \ldots, x_n])^m$ be homogeneous polynomials and $\prec$ be a monomial ordering. There exists a positive integer D for which Gaussian elimination on all $\mathcal{M}^{\mathrm{acaulay}}_{d,m}(f_1, \ldots, f_m)$ matrices for $d, 1 \leq d \leq D$ computes a Gröbner basis of $\langle f_1, \ldots, f_m \rangle$ w.r.t. to $\prec$.

The complexity of computing a Gröbner basis is bounded by the complexity of performing Gaussian elimination on the Macaulay matrices up to some degree D.

Gröbner Bases III

In general, computing the maximum degree in a Gröbner computation is a difficult problem, but is known for a specific family of systems.

Definition (Semi-regular Sequence)

Let $m \geq n$, and $f_1, \ldots, f_m \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be homogeneous polynomials of degrees $d_1, \ldots, d_m$ respectively and $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$. The system is said to be a **semi-regular sequence** if the Hilbert polynomial associated to $\mathcal{I}$ w.r.t. the grevlex order is:

$$\mathrm{HP}(z) = \left[\frac{\prod_{i=1}^{m} (1 - z^{d_i})}{(1 - z)^n} \right]_+ , \tag{2}$$

with $[S]_+$ being the polynomial obtained by truncating the series S before the index of its first non-positive coefficient.

Gröbner Bases IV

Lemma

Let $\mathbf{f} = (f_1, \ldots, f_m) \in (\mathbb{Z}_q[x_1, \ldots, x_n])^m$ *be affine polynomials with* $m > n$. *If* $f_1, \ldots, f_m$ *is semi-regular, then the number of operations in* $\mathbb{Z}_q$ *required to compute a Gröbner basis for any admissible order is bounded by:*

$$\mathcal{O}\left(mD_{reg}\binom{n + D_{reg}}{D_{reg}}^{\omega}\right), \text{ as } D_{reg} \to \infty, \tag{3}$$

where $2 \leq \omega < 3$ *is the linear algebra constant and* D_{reg} *is the* **degree of regularity** *of* $\langle f_1, \ldots, f_m \rangle$*:* $1 + \deg\left(\mathrm{HP}(z)\right)$.

Contents

BinaryError-LWE I

If $\mathbf{e} = (e_1, \ldots, e_m) \in \{0,1\}^m$ and $P(X) = X(X-1)$, then we have $P(e_i) = 0$, for all $i, 1 \leq i \leq m$.

The secret $\mathbf{s} \in \mathbb{Z}_q^n$ is a solution to:

$$f_1 = P\big(c_1 - \sum_{j=1}^{n} s_j G_{j,1}\big) = 0, \; \ldots, \; f_m = P\big(c_n - \sum_{j=1}^{n} s_j G_{j,n}\big) = 0. \qquad (4)$$

This is an algebraic system of m quadratic equations in $\mathbb{Z}_q[x_1, \ldots, x_n]$.

BinaryError-LWE II

We make the following assumption about the structure of the generated polynomials:

Assumption

Let $(G, \mathbf{s} \times G + \mathbf{e}) = (G, \mathbf{c}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ *be sampled according to* $L^{(n)}_{\mathbf{s}, \mathcal{U}(\mathbb{F}_2)}$, *and let* $P(x) = X(X-1)$. *We define:*

$$f_1 = P\big(c_1 - \sum_{j=1}^{n} s_j G_{j,1}\big) = 0, \ \ldots\ , f_m = P\big(c_n - \sum_{j=1}^{n} s_j G_{j,m}\big) = 0.$$

It holds that $\langle f_1, \ldots, f_m \rangle$ *is semi-regular.*

BinaryError-LWE III

Theorem

(i) *Let $m = C \cdot n$, with $C > 1$, and let $f_1, \ldots, f_m \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a semi-regular system of equations. The degree of regularity of $f_1, \ldots, f_m$ behaves asymptotically as*

$$D_{\mathrm{reg}} = \left(C - \frac{1}{2} - \sqrt{C(C-1)}\right) n - \frac{a_1}{2\big(C(C-1)\big)^{1/6}} n^{\frac{1}{3}} - \left(2 - \frac{2C-1}{4\big(C(C-1)\big)^{1/2}}\right) + \mathcal{O}\left(\frac{1}{n^{\frac{1}{3}}}\right),$$

where $a_1 \approx 2.3381$ is the largest zero of the classical Airy function.

(ii) *Let $m = n \cdot \log^{1/\epsilon}(n)$, for any constant $\epsilon > 0$, or $m = n \log \log n$. The degree of regularity of $f_1, \ldots, f_m$ behaves asymptotically as:*

$$D_{\mathrm{reg}} = \frac{n^2}{8m}\left(1 + o(1)\right).$$

BinaryError-LWE IV

Theorem

Let $\omega, 2 \leq \omega < 3$, be the linear algebra constant. Under our assumption:

(i) *If $m = n\left(1 + \frac{1}{\log(n)}\right)$, then there is an algorithm solving* BinaryError-LWE *in*

$$\mathcal{O}\left(n^2\, 2^{1.37\,\omega\, n}\right) \text{ operations.}$$

...

(iv) *If $m = \mathcal{O}\left(n \log\log n\right)$, in*

$$\mathcal{O}\left(m^2\, 2^{\frac{\omega\; n\; \log\log\log n}{8\log\log n}}\right) \text{ operations.}$$

Summary

- Given access to $m \geq 6.6\, n$ samples we can solve BinaryError-LWE in time
$$\mathcal{O}\left(n^2\, 2^{0.344\, n}\right)$$
- Given access to $m = \mathcal{O}\left(n \log\log n\right)$ samples we can solve BinaryError-LWE in **subexponential** time:
$$\mathcal{O}\left(2^{\frac{\omega\, n\, \log\log\log n}{8 \log\log n}}\right).$$

Contents

Arora-GB I

To analyse the complexity of solving LWE with Arora-Ge and Gröbner bases, we make use of the following simple technical lemma:

Lemma

Let $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_m, b_m)$ *be elements of* $\mathbb{F}_q^n \times \mathbb{F}_q$ *sampled according to* $\mathrm{LWE}_{\chi_{\alpha,q}}$. *If* $C = \sqrt{2\log(m)}$ *then, the equations generated as in* (1) *vanish with probability at least:*

$$p_{\mathrm{g}} = 1 - \sqrt{\frac{1}{\pi \cdot \log(m)}}.$$

Arora-GB II

We assume that $\sigma = n^{\epsilon}$, with $0 \leq \theta \leq \epsilon \leq 1$. We consider a number of samples of the following form:

$$M_{\mathrm{GB}} = e^{\gamma_\theta}, \text{ with } \gamma_\theta = n^{2\cdot(\epsilon-\theta)}.$$

Note that $\theta = 0$ corresponds up to polylog factors to the basic Arora-Ge approach.

Arora-GB III

We can then deduce the degree D_{GB} required for $M_{\mathrm{GB}} = e^{\gamma_\theta}$ equations. We have to fix $C_{\mathrm{GB}} = \sqrt{2 \cdot \log(M_{\mathrm{GB}})} = \sqrt{2 \cdot \gamma_\theta}$, giving us:

$$\begin{aligned} D_{\mathrm{GB}} &= 2\sqrt{2 \cdot \log(M_{\mathrm{GB}})} \cdot \sigma + 1 \in \mathcal{O}\left(\sqrt{\log(M_{\mathrm{GB}})} \cdot \sigma\right) \\ &= \mathcal{O}\left(\sqrt{\gamma_\theta} \cdot \sigma\right) = \mathcal{O}\left(n^{2\epsilon-\theta}\right) = \mathcal{O}\left(\gamma_\theta \cdot n^\theta\right). \end{aligned}$$

But to ease the analysis below, we further simplify D_{GB} to:

$$D_{\mathrm{GB}} \approx \gamma_\theta \cdot n^\theta = \log(M_{\mathrm{GB}}) \cdot n^\theta.$$

Arora-GB IV

Again, our results depend crucially on an assumption about the structure of the generated equations:

Assumption

Let $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_{M_{\mathrm{GB}}}, b_{M_{\mathrm{GB}}})$ *be elements of* $\mathbb{F}_q^n \times \mathbb{F}_q$ *sampled according to* $\mathrm{LWE}_{\chi_{\alpha,q}}$*. Let* $P(X) = X \prod_{i=1}^{C_{\mathrm{GB}} \cdot \sigma} (X+i)(X-i)$*. We define:*

$$f_i = P\Big(-b + \sum_{j=1}^{n} (\mathbf{a}_i)_{(j)} x_j\Big) = 0, \forall i, 1 \leq i \leq M_{\mathrm{GB}}. \qquad (7)$$

Then, $\langle f_1, \ldots, f_m \rangle$ *is semi-regular.*

Arora-GB V

From D_{GB} and M_{GB} we now need to establish the degree of regularity.

Lemma

Let $A \geq 1$, and $f_1, \ldots, f_m \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be semi-regular polynomials of degree $\frac{n}{A}$, and D_{reg} be the degree of regularity of these polynomials. If $m = e^{\frac{\pi \cdot n}{4 \cdot A^2}}$, then it holds that D_{reg} behaves asymptotically as

$$C_A \cdot n, \text{where } C_A \text{ is a constant which depends on } A.$$

Complexity

Arora-Ge (Linearisation) with $\sigma = \sqrt{n}$

$$\mathcal{O}\left(2^{8\,\omega\, n \log n(\log n - \log(8\, n \log n))}\right)$$

Gröbner Bases with $\sigma = \sqrt{n}$

$$\mathcal{O}\left(2^{n\left(2.35\,\omega + 1.13\right)}\right)$$

under some regularity assumption.

Contents

Fröberg's Conjecture I

- Our results depend on two similar assumptions, i.e. that our systems behave like semi-regular sequences.
- We cannot prove that this holds.
- We **experimentally** verified our assumptions for up to non-trivial problem sizes.
- We note that our assumptions are related to a famous conjecture in algebraic geometry known as **Fröberg's conjecture**.
- It states that that a property – i.e. the rank of some linear map associated to Macaulay matrices is maximal – holds **generically**.
- Genericity means that a property holds except for the vanishing set of some polynomial.

Fröberg's Conjecture II

- A matrix has full rank if its determinant is not zero.
- Matrices have full rank except when their determinant polynomial vanishes.
- This happens with low probability by the Schwartz - Zippel - DeMillo - Lipton lemma:

Lemma (Schwartz, Zippel, DeMillo, Lipton)

Let $\mathbb{K}$ be a field and $P \in \mathbb{K}[x_1, \ldots, x_n]$ be a non-zero polynomial. Select $r_1, \ldots, r_n$ uniformly at random from a finite subset $\mathcal{X}$ of $\mathbb{K}$. Then, the probability that $P(r_1, \ldots, r_n) = 0$ is less than $\deg(P)/|\mathcal{X}|$.

Fröberg's Conjecture III

- The main difficulty in Fröberg's conjecture is to prove that the determiant polynomial is not always identically zero.
- If you try a random example, it will almost always work. But what about as n goes to infinity?
- To prove Fröberg's conjecture, we must find **one** explicit family of equations for which we can be proven semi-regular for any m and n.

Fröberg's Conjecture IV

- Proving our assumptions would provide such family and hence solve Fröberg's conjecture.
- Furthermore, any non-trivial partial results on our assumptions would lead to progress on the general Fröberg's conjecture.
- Indeed, Fröberg and Hollman already investigated the genericity of squares of linear forms, i.e. a problem very close to ours, in order to make progress on Fröberg's conjecture.

We report some progress towards proving Fröberg conjecture by investigating our assumptions. We prove

- that the equations $f_1, \ldots, f_m$ generated for BinaryError-LWE are linearly independent with high probability;
- that for BinaryError-LWE $f_1, \ldots, f_m$ with $m \leq n + \lfloor \frac{n-2}{2} \rfloor$ is semigeneric, i.e. $\{x_i \cdot f_j\}_{1 \leq i \leq n}^{1 \leq j \leq n}$ spans a vector space of maximal dimension;
- that the assumption holds for BinaryError-LWE for $m = n + 1$ and a sufficiently big field.

An Example I

Lemma

For all $i, 1 \leq i \leq n$*, construct a* $n \times \big(n-(i-1)\big)$ *matrix* G_i *as follows. All the coefficients of* G_i *are zero except:*

- $G_i[i,j] = 1$*, for all* $j, 1 \leq j \leq \big(n-(i-1)\big)$.
- $G_i[j+(i-1),j] = 1$*, for all* $j, 1 \leq j \leq \big(n-(i-1)\big)$.

Now, let $G^* = G_1 \| G_2 \| \cdots \| G_n$ *be a block matrix,* $\mathbf{s} \in \mathbb{Z}_q^n$ *chosen uniformly at random, and* $\mathbf{e} \in \{0,1\}^m$ *sampled uniformly. We set* $\mathbf{c} = \mathbf{s} \times G^* + \mathbf{e}$ *and* $P(x) = X(X-1)$ *and define:*

$$f_1 = P\big(c_1 - \sum_{j=1}^{n} x_j G^*_{j,1}\big), \quad \ldots \quad , f_m = P\big(c_m - \sum_{j=1}^{n} x_j G^*_{j,m}\big).$$

Then, the homogeneous components $f_1^{\mathrm{H}}, \ldots, f_m^{\mathrm{H}}$ *of degree* 2 *are linearly independent.*

An Example II

For $n = 4$, and $m = n(n+1)/2 = 10$ the matrix G^* is as follows:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & \\ & 1 & & & 1 & 1 & 1 & & & \\ & & 1 & & & 1 & & 1 & 1 & \\ & & & 1 & & & 1 & & 1 & 1 \end{bmatrix}.$$

An Example III

The generated equations are

$$
\begin{aligned}
0 &= x_1^2 + 15 \cdot x_1 + 5, \\
0 &= x_1^2 + 2 \cdot x_1 \cdot x_2 + x_2^2 + 4, \\
0 &= x_1^2 + 2 \cdot x_1 \cdot x_3 + x_3^2 + 10 \cdot x_1 + 10 \cdot x_3 + 12, \\
0 &= x_1^2 + 2 \cdot x_1 \cdot x_4 + x_4^2 + 9 \cdot x_1 + 9 \cdot x_4 + 3, \\
0 &= x_2^2 + 5 \cdot x_2 + 6, \\
0 &= x_2^2 + 2 \cdot x_2 \cdot x_3 + x_3^2 + 4, \\
0 &= x_2^2 + 2 \cdot x_2 \cdot x_4 + x_4^2 + 16 \cdot x_2 + 16 \cdot x_4, \\
0 &= x_3^2 + 13 \cdot x_3 + 8, \\
0 &= x_3^2 + 2 \cdot x_3 \cdot x_4 + x_4^2 + 7 \cdot x_3 + 7 \cdot x_4 + 12, \\
0 &= x_4^2 + 14 \cdot x_4 + 2.
\end{aligned}
$$

An Example IV

By performing the reductions, we get:

$$\begin{aligned}
0 &= \mathbf{x_1^2} + 15 \cdot x_1 + 5, \\
0 &= \mathbf{2 \cdot x_1 \cdot x_2} + x_2^2 + 2 \cdot x_1 + 16, \\
0 &= \mathbf{2 \cdot x_1 \cdot x_3} + x_3^2 + 12 \cdot x_1 + 10 \cdot x_3 + 7, \\
0 &= \mathbf{2 \cdot x_1 \cdot x_4} + x_4^2 + 11 \cdot x_1 + 9 \cdot x_4 + 15, \\
0 &= \mathbf{x_2^2 + 5 \cdot x_2} + 6, \\
0 &= \mathbf{2 \cdot x_2 \cdot x_3} + x_3^2 + 12 \cdot x_2 + 15, \\
0 &= \mathbf{2 \cdot x_2 \cdot x_4} + x_4^2 + 11 \cdot x_2 + 16 \cdot x_4 + 11, \\
0 &= \mathbf{x_3^2} + 13 \cdot x_3 + 8, \\
0 &= \mathbf{2 \cdot x_3 \cdot x_4} + x_4^2 + 11 \cdot x_3 + 7 \cdot x_4 + 4, \\
0 &= \mathbf{x_4^2} + 14 \cdot x_4 + 2
\end{aligned}$$

Fin

Questions?