On the Existence of Semi-Regular Sequences

Sergio Molina[1]
joint work with
T. J. Hodges[1] J. Schlather

[1]Department of Mathematics
University of Cincinnati

DIMACS, January 2015

Background

- Important Problem: Finding solutions to systems of polynomial equations of the form

$$p_1(x_1, \ldots, x_n) = \beta_1, \ldots, p_m(x_1, \ldots, x_n) = \beta_m. \tag{1}$$

Background

- Important Problem: Finding solutions to systems of polynomial equations of the form

$$p_1(x_1, \ldots, x_n) = \beta_1, \ldots, p_m(x_1, \ldots, x_n) = \beta_m. \tag{1}$$

- MPKC systems: Multivariate Public Key Cryptographic systems.

Background

- Important Problem: Finding solutions to systems of polynomial equations of the form

$$p_1(x_1, \ldots, x_n) = \beta_1, \ldots, p_m(x_1, \ldots, x_n) = \beta_m. \tag{1}$$

- MPKC systems: Multivariate Public Key Cryptographic systems.
- The security of MPKC systems relies on the difficulty of solving a system (1) of quadratic equations over a finite field.

Background

- Main types of algorithms used to solve such systems of equations are:

Background

- Main types of algorithms used to solve such systems of equations are:
- Gröbner basis algorithm [Buchberger] and its variants $\mathbf{F}_4$ and $\mathbf{F}_5$ [Faugère].

Background

- Main types of algorithms used to solve such systems of equations are:
- Gröbner basis algorithm [Buchberger] and its variants $\mathbf{F}_4$ and $\mathbf{F}_5$ [Faugère].
- The **XL** algorithms including **FXL** [Courtois et al.] and **mutantXL** [Buchmann et al.].

Background

- To assess complexity of the $\mathbf{F}_4$ and $\mathbf{F}_5$ algorithms for solution of polynomial equations the concept of "semi-regular" sequences over $\mathbb{F}_2$ was introduced by Bardet, Faugère, Salvy and Yang.

Background

- To assess complexity of the $\mathbf{F}_4$ and $\mathbf{F}_5$ algorithms for solution of polynomial equations the concept of "semi-regular" sequences over $\mathbb{F}_2$ was introduced by Bardet, Faugère, Salvy and Yang.
- Roughly speaking, semi-regular sequences over $\mathbb{F}_2$ are sequences of homogeneous elements of the algebra

$$B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$$

which have as few relations between them as possible.

Background

- To assess complexity of the $\mathbf{F}_4$ and $\mathbf{F}_5$ algorithms for solution of polynomial equations the concept of "semi-regular" sequences over $\mathbb{F}_2$ was introduced by Bardet, Faugère, Salvy and Yang.
- Roughly speaking, semi-regular sequences over $\mathbb{F}_2$ are sequences of homogeneous elements of the algebra

$$B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$$

  which have as few relations between them as possible.
- Experimental evidence has shown that randomly generated sequences tend to be semi-regular.

Definitions

Let $B_d \subset B^{(n)}$ be the set of homogeneous polynomials of degree d.

Definitions

Let $B_d \subset B^{(n)}$ be the set of homogeneous polynomials of degree d.

Definition 1

Let $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$. If $\lambda_1, ..., \lambda_m \in B^{(n)}$ is a sequence of homogeneous elements of positive degrees $d_1, ..., d_m$ and $I = (\lambda_1, ..., \lambda_m)$ then

Definitions

Let $B_d \subset B^{(n)}$ be the set of homogeneous polynomials of degree d.

Definition 1

Let $B^{(n)} = \mathbb{F}_2[X_1, \dots, X_n]/(X_1^2, \dots, X_n^2)$. If $\lambda_1, \dots, \lambda_m \in B^{(n)}$ is a sequence of homogeneous elements of positive degrees $d_1, \dots, d_m$ and $I = (\lambda_1, \dots, \lambda_m)$ then

- $\operatorname{Ind}(I) = \min\{d \geq 0 \mid I \cap B_d = B_d\}$

Definitions

Let $B_d \subset B^{(n)}$ be the set of homogeneous polynomials of degree d.

Definition 1

Let $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$. If $\lambda_1, ..., \lambda_m \in B^{(n)}$ is a sequence of homogeneous elements of positive degrees $d_1, ..., d_m$ and $I = (\lambda_1, ..., \lambda_m)$ then

- $\mathrm{Ind}(I) = \min\{d \geq 0 \mid I \cap B_d = B_d\}$
- The sequence $\lambda_1, \ldots, \lambda_m$ is **semi-regular** over $\mathbb{F}_2$ if for all $i = 1, 2, \ldots, m$, if μ is homogeneous and

$$\mu\lambda_i \in (\lambda_1, \ldots, \lambda_{i-1}) \quad \text{and} \quad \deg(\mu) + \deg(\lambda_i) < \mathrm{Ind}(I)$$

then $\mu \in (\lambda_1, \ldots, \lambda_i)$.

Characterization with Hilbert Series

Characterization with Hilbert Series

- The truncation of a series $\sum a_i z^i$ is defined to be:

$$\left[\sum a_i z^i\right] = \sum b_i z^i$$

where $b_i = a_i$ if $a_j > 0$ for all $j \leq i$, and $b_i = 0$ otherwise.

Characterization with Hilbert Series

- The truncation of a series $\sum a_i z^i$ is defined to be:

$$\left[\sum a_i z^i\right] = \sum b_i z^i$$

where $b_i = a_i$ if $a_j > 0$ for all $j \leq i$, and $b_i = 0$ otherwise.

- For instance

$$[1 + 10z + z^2 + 20z^3 - z^4 + z^6 + \cdots] = 1 + 10z + z^2 + 20z^3$$

Characterization with Hilbert Series

Theorem 2 (Bardet, Faugère, Salvy, Yang)

Let $\lambda_1, ..., \lambda_m \in B^{(n)}$ be a sequence of homogeneous elements of positive degrees $d_1, ..., d_m$ and $I = (\lambda_1, ..., \lambda_m)$. Then, the sequence $\lambda_1, ..., \lambda_m$ is semi-regular if and only if

$$Hilb_{B^{(n)}/I}(z) = \left[\frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})} \right]$$

Characterization with Hilbert Series

Theorem 2 (Bardet, Faugère, Salvy, Yang)

Let $\lambda_1, ..., \lambda_m \in B^{(n)}$ be a sequence of homogeneous elements of positive degrees $d_1, ..., d_m$ and $I = (\lambda_1, ..., \lambda_m)$. Then, the sequence $\lambda_1, ..., \lambda_m$ is semi-regular if and only if

$$Hilb_{B^{(n)}/I}(z) = \left[\frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})} \right]$$

- Let $\lambda_1, ..., \lambda_m \in B^{(n)}$ be a sequence of homogeneous elements and let $I = (\lambda_1, ..., \lambda_m)$. If the sequence is semi-regular then

$$\mathrm{Ind}(\lambda_1, ..., \lambda_m) = 1 + \deg(Hilb_{B^{(n)}/I}(z))$$

Example

- Consider the element $\lambda = x_1x_2 + x_3x_4 + x_5x_6$ in $B^{(6)}$ and let $I = (\lambda)$.

Example

- Consider the element $\lambda = x_1x_2 + x_3x_4 + x_5x_6$ in $B^{(6)}$ and let $I = (\lambda)$.
- $$HS_{B^{(6)}/I}(z) = 1 + 6z + 14z^2 + 14z^3 + z^4$$

  and
  $$\frac{(1+z)^6}{1+z^2} = 1 + 6z + 14z^2 + 14z^3 + z^4 - 8z^5 + \cdots$$

Example

- Consider the element $\lambda = x_1x_2 + x_3x_4 + x_5x_6$ in $B^{(6)}$ and let $I = (\lambda)$.
- $$HS_{B^{(6)}/I}(z) = 1 + 6z + 14z^2 + 14z^3 + z^4$$

  and
  $$\frac{(1+z)^6}{1+z^2} = 1 + 6z + 14z^2 + 14z^3 + z^4 - 8z^5 + \cdots$$
- $\left[\frac{(1+z)^6}{1+z^2}\right] = 1 + 6z + 14z^2 + 14z^3 + z^4 = HS_{B^{(6)}/I}(z)$.

Example

- Consider the element $\lambda = x_1x_2 + x_3x_4 + x_5x_6$ in $B^{(6)}$ and let $I = (\lambda)$.
- $$HS_{B^{(6)}/I}(z) = 1 + 6z + 14z^2 + 14z^3 + z^4$$
  and
  $$\frac{(1+z)^6}{1+z^2} = 1 + 6z + 14z^2 + 14z^3 + z^4 - 8z^5 + \cdots$$
- $\left[\frac{(1+z)^6}{1+z^2}\right] = 1 + 6z + 14z^2 + 14z^3 + z^4 = HS_{B^{(6)}/I}(z)$.
- λ is semi-regular and $\mathrm{Ind}(\lambda) = 5$.

Existence of Semi-Regular Sequences

- Sequences that are trivially semi-regular:

Existence of Semi-Regular Sequences

- Sequences that are trivially semi-regular:
- Sequences of linear elements that are linearly independent are semi-regular.

Existence of Semi-Regular Sequences

- Sequences that are trivially semi-regular:
- Sequences of linear elements that are linearly independent are semi-regular.
- Sequences of homogeneous polynomials of degree $n-1$ in $B^{(n)}$ that are linearly independent are semi-regular.

Existence of Semi-Regular Sequences

- Sequences that are trivially semi-regular:
- Sequences of linear elements that are linearly independent are semi-regular.
- Sequences of homogeneous polynomials of degree $n-1$ in $B^{(n)}$ that are linearly independent are semi-regular.
- $x_1 x_2 \cdots x_n \in B^{(n)}$ is semi-regular.

Existence of Semi-Regular Sequences

- Sequences that are trivially semi-regular:
- Sequences of linear elements that are linearly independent are semi-regular.
- Sequences of homogeneous polynomials of degree $n-1$ in $B^{(n)}$ that are linearly independent are semi-regular.
- $x_1 x_2 \cdots x_n \in B^{(n)}$ is semi-regular.
- Any a basis of B_d the space of homogeneous polynomials of degree d, is semi-regular.

Existence of Semi-Regular Sequences

Conjecture 1 (Bardet, Faugère, Salvy, Yang)

The proportion of semi-regular sequences tends to one as the number of variables tends to infinity.

Existence of Semi-Regular Sequences

Conjecture 1 (Bardet, Faugère, Salvy, Yang)

The proportion of semi-regular sequences tends to one as the number of variables tends to infinity.

- This conjecture is true in the following precise sense.

Existence of Semi-Regular Sequences

Conjecture 1 (Bardet, Faugère, Salvy, Yang)

The proportion of semi-regular sequences tends to one as the number of variables tends to infinity.

- This conjecture is true in the following precise sense.

Theorem 3 (Hodges, Molina, Schlather)

Let $h(n)$ be the number of subsets of $B^{(n)}$ consisting of homogeneous elements of degree greater than or equal to one. Let $s(n)$ be the number of such subsets that are semi-regular. Then

$$\lim_{n\to\infty} \frac{s(n)}{h(n)} = 1$$

Non-Existence of Semi-Regular Sequences

Conjecture 2 (Bardet, Faugère, Salvy)

Let $\pi(n, m, d_1, \ldots, d_m)$ be the proportion of sequences in $B^{(n)}$ of m elements of degrees $d_1, \ldots, d_m$ that are semi-regular. Then $\pi(n, m, d_1, \ldots, d_m)$ tends to 1 as n tends to ∞.

Non-Existence of Semi-Regular Sequences

Conjecture 2 (Bardet, Faugère, Salvy)

Let $\pi(n, m, d_1, \ldots, d_m)$ be the proportion of sequences in $B^{(n)}$ of m elements of degrees $d_1, \ldots, d_m$ that are semi-regular. Then $\pi(n, m, d_1, \ldots, d_m)$ tends to 1 as n tends to ∞.

- This conjecture is false. In fact the opposite is true.

Non-Existence of Semi-Regular Sequences

Conjecture 2 (Bardet, Faugère, Salvy)

Let $\pi(n, m, d_1, \ldots, d_m)$ be the proportion of sequences in $B^{(n)}$ of m elements of degrees $d_1, \ldots, d_m$ that are semi-regular. Then $\pi(n, m, d_1, \ldots, d_m)$ tends to 1 as n tends to ∞.

- This conjecture is false. In fact the opposite is true.

Theorem 4 (Hodges, Molina, Schlather)

For a fixed choice of $(m, d_1, \ldots, d_m)$*, there exists* N *such that*

$$\pi(n, m, d_1, \ldots, d_m) = 0.$$

for all $n \geq N$*.*

Table: Proportion of Samples of 20 Sets of m Homogeneous Quadratic Elements in n variables that are Semi-Regular

$n \backslash m$	2	3	4	5	6	7	8	9	10	11	12	13	14
3	1	.8	1	1	1	1							
4	.35	1	.75	.75	.3	.65	.85	.9	1	1	1	1	1
5	0	.85	.95	1	.9	.85	.75	.6	.2	.65	.7	.9	.9
6	.85	.7	.65	.9	1	1	1	.95	.95	.95	.75	.8	.5
7	0	.85	1	.1	1	1	1	1	1	1	1	.95	1
8	.7	.45	1	1	.95	.1	1	1	1	1	1	1	1
9	0	.95	.7	1	1	1	1	.8	.9	1	1	1	1
10	0	.85	1	.35	1	1	1	1	1	1	.25	1	1
11	0	.95	1	1	1	1	1	1	1	1	1	1	1
12	0	0	1	1	1	1	.9	1	1	1	1	1	1
13	0	0	1	1	1	1	1	1	1	1	1	1	1
14	0	0	0	1	1	1	1	1	1	1	1	1	1
15	0	0	0	1	1	1	1	1	1	1	1	1	.45

- Neither of the previous conjectures accurately addresses the observed fact that "most" quadratic sequences of length n in n variables are semi-regular.

- Neither of the previous conjectures accurately addresses the observed fact that “most” quadratic sequences of length n in n variables are semi-regular.

Conjecture 3

For any $1 \leq d \leq n$ define $\pi(n, d)$ to be the proportion of sequences of degree d and length n in n variables that are semi-regular. Then

$$\lim_{n \to \infty} \pi(n, d) = 1.$$

- Neither of the previous conjectures accurately addresses the observed fact that "most" quadratic sequences of length n in n variables are semi-regular.

Conjecture 3

For any $1 \leq d \leq n$ define $\pi(n, d)$ to be the proportion of sequences of degree d and length n in n variables that are semi-regular. Then

$$\lim_{n \to \infty} \pi(n, d) = 1.$$

Conjecture 4

There exists an ϵ such that if $m(n) = \lfloor \alpha n \rfloor + c$, then the proportion of sequences of length $m(n)$ in n variables tends to one as n tends to infinity whenever $\alpha > \epsilon$.

Existence of Semi-Regular Sequences (case $m = 1$)

Question 1

For which values of n and d do there exist semi-regular elements of degree d in $B^{(n)}$?

Existence of Semi-Regular Sequences (case $m = 1$)

Question 1

For which values of n and d do there exist semi-regular elements of degree d in $B^{(n)}$?

- In her thesis Bardet asserts that the elementary symmetric quadratic polynomial

$$\sigma_2(x_1, ..., x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$$

is semi-regular for all n.

Existence of Semi-Regular Sequences (case $m = 1$)

Question 1

For which values of n and d do there exist semi-regular elements of degree d in $B^{(n)}$?

- In her thesis Bardet asserts that the elementary symmetric quadratic polynomial

$$\sigma_2(x_1, ..., x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$$

  is semi-regular for all n.
- By the previous theorem there are finitely many values of n for which $\sigma_2(x_1, ..., x_n)$ can be semi-regular. Moreover, we have the following theorem.

Existence of Semi-Regular Sequences (case $m = 1$)

Theorem 5 (Hodges, Molina, Schlather)

A homogeneous element of degree $d \geq 2$ can only be semi-regular if $n \leq 3d$.

Existence of Semi-Regular Sequences (case $m = 1$)

Theorem 5 (Hodges, Molina, Schlather)

A homogeneous element of degree $d \geq 2$ can only be semi-regular if $n \leq 3d$.

- For instance $\sigma_2(x_1, ..., x_n)$ (or any quadratic homogeneous polynomial) can only be semi-regular if $n \leq 6$.

Existence of Semi-Regular Sequences (case $m = 1$)

Theorem 5 (Hodges, Molina, Schlather)

A homogeneous element of degree $d \geq 2$ can only be semi-regular if $n \leq 3d$.

- For instance $\sigma_2(x_1, ..., x_n)$ (or any quadratic homogeneous polynomial) can only be semi-regular if $n \leq 6$.
- Is the bound $n = 3d$ sharp?

Existence of Semi-Regular Sequences (case $m = 1$)

Theorem 6 (Hodges, Molina, Schlather)

Let $d \geq 2$, where $d = 2^k l$ with l an odd number, and k a non-negative integer. Consider the elementary symmetric polynomial of degree d

$$\sigma_{d,n} = \sum_{1 \leq i_1 < \cdots < i_d \leq n} x_{i_1} \cdots x_{i_d}$$

then

(a) *If $l > 1$, $\sigma_{d,n}$ is semi-regular if and only if $d \leq n \leq d + 2^{k+1} - 1$.*

(b) *If $l = 1$, $\sigma_{d,n}$ is semi-regular if and only if $d \leq n \leq d + 2^{k+1}$.*

Existence of Semi-Regular Sequences (case $m = 1$)

Theorem 6 (Hodges, Molina, Schlather)

Let $d \geq 2$, where $d = 2^k l$ with l an odd number, and k a non-negative integer. Consider the elementary symmetric polynomial of degree d

$$\sigma_{d,n} = \sum_{1 \leq i_1 < \cdots < i_d \leq n} x_{i_1} \cdots x_{i_d}$$

then

(a) *If $l > 1$, $\sigma_{d,n}$ is semi-regular if and only if $d \leq n \leq d + 2^{k+1} - 1$.*

(b) *If $l = 1$, $\sigma_{d,n}$ is semi-regular if and only if $d \leq n \leq d + 2^{k+1}$.*

- In particular when $d = 2^k$, $\sigma_{d,n}$ is semi-regular for all $d \leq n \leq 3d$, thus establishing that the bound is sharp for infinitely many n.

$n\backslash d$	2	3	4	5	6	7	8	9	10	11	12	13	14
2	x												
3	x	x											
4	x	x	x										
5	x		x	x									
6	x		x	x	x								
7			x		x	x							
8			x		x	x	x						
9			x		x		x	x					
10			x				x	x	x				
11			x				x		x	x			
12			x				x		x	x	x		
13							x		x		x	x	
14							x				x	x	x

Table: Semi-Regularity of $\sigma_{d,n}$. The values when $\sigma_{d,n}$ is semi-regular are marked with an x

Example

- For $n = 50$ variables the following elements are semi-regular:

Example

- For $n = 50$ variables the following elements are semi-regular:
- Any element of degree $d = 1$, $d = 49$ or $d = 50$ is trivially semi-regular.

Example

- For $n = 50$ variables the following elements are semi-regular:
- Any element of degree $d = 1$, $d = 49$ or $d = 50$ is trivially semi-regular.
- The elementary symmetric polynomial of degree d, $\sigma_d(x_1, \ldots, x_{50})$ is semi-regular for $d = 32, 44, 48$.

- We need to prove the observed fact that "most" quadratic sequences are semi-regular.

- We need to prove the observed fact that “most” quadratic sequences are semi-regular.
- Even the question of the existence of quadratic sequences of length n in n variables for all n remains open.

Thank you very much!

Thank you very much!

T. Hodges, S. Molina, J. Schlather, *On the Existence of Semi-Regular Sequences*. Available under `http://arxiv.org/abs/1412.7865`