Mathematical Problems in Multivariate Public Key Cryptography

Timothy Hodges

University of Cincinnati

January 15, 2015

Overview

Outline

1. Multivariate Public Key Cryptosystems
2. Solving Systems of Polynomial Equations
3. First Fall Degree and HFE-systems
4. Semi-regular systems

Multivariate Public Key Cryptosystems

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

$$\mathbb{F}^n \xrightarrow{\{p_1,\dots,p_n\}} \mathbb{F}^m$$

$p_i(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]/\left\langle x_1^q - x_1, \dots, x_n^q - x_n \right\rangle = \mathrm{Fun}(\mathbb{F}^n, \mathbb{F})$

Solving

$$\begin{aligned} p_1(x_1, \dots, x_n) &= y_1 \\ \vdots \quad & \quad \vdots \\ p_m(x_1, \dots, x_n) &= y_m \end{aligned}$$

is a hard problem.

Problem

Design a trapdoor that retains this level of security.

Multivariate Public Key Cryptosystems

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

$$\mathbb{F}^n \xrightarrow{\{p_1,\dots,p_n\}} \mathbb{F}^m$$

$p_i(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n] / \langle x_1^q - x_1, \dots, x_n^q - x_n \rangle = \mathrm{Fun}(\mathbb{F}^n, \mathbb{F})$

Solving

$$\begin{aligned} p_1(x_1, \dots, x_n) &= y_1 \\ \vdots \quad &\quad \vdots \\ p_m(x_1, \dots, x_n) &= y_m \end{aligned}$$

is a hard problem.

Problem

Design a trapdoor that retains this level of security.

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

$$\mathbb{F}^n \xrightarrow{\{p_1,\ldots,p_n\}} \mathbb{F}^m$$

$$p_i(x_1,\ldots,x_n) \in \mathbb{F}[x_1,\ldots,x_n]/\left\langle x_1^q - x_1,\ldots,x_n^q - x_n\right\rangle = \mathrm{Fun}(\mathbb{F}^n,\mathbb{F})$$

Solving

$$\begin{aligned} p_1(x_1,\ldots,x_n) &= y_1 \\ \vdots \quad &\quad \vdots \\ p_m(x_1,\ldots,x_n) &= y_m \end{aligned}$$

is a hard problem.

Problem

Design a trapdoor that retains this level of security.

Multivariate Public Key Cryptosystems

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

$$\mathbb{F}^n \xrightarrow{\{p_1,\dots,p_n\}} \mathbb{F}^m$$

$p_i(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]/\left\langle x_1^q - x_1, \dots, x_n^q - x_n \right\rangle = \mathrm{Fun}(\mathbb{F}^n, \mathbb{F})$

Solving

$$\begin{aligned} p_1(x_1, \dots, x_n) &= y_1 \\ \vdots \quad &\quad \vdots \\ p_m(x_1, \dots, x_n) &= y_m \end{aligned}$$

is a hard problem.

Problem

Design a trapdoor that retains this level of security.

Multivariate Public Key Cryptosystems

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

$$\mathbb{F}^n \xrightarrow{\{p_1,\ldots,p_n\}} \mathbb{F}^m$$

$$p_i(x_1,\ldots,x_n) \in \mathbb{F}[x_1,\ldots,x_n]/\left\langle x_1^q - x_1,\ldots,x_n^q - x_n\right\rangle = \mathrm{Fun}(\mathbb{F}^n,\mathbb{F})$$

Solving

$$\begin{aligned} p_1(x_1,\ldots,x_n) &= y_1 \\ \vdots \quad &\quad \vdots \\ p_m(x_1,\ldots,x_n) &= y_m \end{aligned}$$

is a hard problem.

Problem

Design a trapdoor that retains this level of security.

Hidden Field Systems: Matsumoto-Imai

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t}\alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "P"] & \mathbb{K} \arrow[d, "\tau"] \\
\mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1,\ldots,p_n\}"] & \mathbb{F}^n
\end{tikzcd}$$

Private Key

Public Key

σ, τ invertible affine linear maps

Hidden Field Systems: Matsumoto-Imai

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t}\alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "P"] & \mathbb{K} \arrow[d, "\tau"] \\
\mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1,\dots,p_n\}"] & \mathbb{F}^n
\end{tikzcd}$$

Private Key

Public Key

σ, τ invertible affine linear maps

Hidden Field Systems: Matsumoto-Imai

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t}\alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$$\begin{tikzcd} \mathbb{K} \arrow[r, "P"] & \mathbb{K} \arrow[d, "\tau"] \\ \mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1, \dots, p_n\}"] & \mathbb{F}^n \end{tikzcd}$$

Private Key

Public Key

σ, τ invertible affine linear maps

Hidden Field Systems: Matsumoto-Imai

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t}\alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "P"] & \mathbb{K} \arrow[d, "\tau"] \\
\mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1,\dots,p_n\}"] & \mathbb{F}^n
\end{tikzcd}$$

Private Key

Public Key

σ, τ invertible affine linear maps

Hidden Field Systems: Matsumoto-Imai

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^{\theta}$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^{\theta})^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t}\alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$$\begin{tikzcd} \mathbb{K} \arrow[r, "P"] & \mathbb{K} \arrow[d, "\tau"] \\ \mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1,\dots,p_n\}"] & \mathbb{F}^n \end{tikzcd}$$

Private Key

Public Key

σ, τ invertible affine linear maps

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^{\theta}$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^{\theta})^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t}\alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$$\begin{tikzcd} \mathbb{K} \arrow[r, "P"] & \mathbb{K} \arrow[d, "\tau"] \\ \mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1,\dots,p_n\}"] & \mathbb{F}^n \end{tikzcd}$$

Private Key

Public Key

σ, τ invertible affine linear maps

Patarin's HFE System

$P(X)$ is

- of low total degree, D (efficient decryption).
- quadratic over $\mathbb{F}$ so that $p_i(x_1, \ldots, x_n)$ are quadratic (efficient encryption)

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "P(X)"] & \mathbb{K} \arrow[d, "\tau"] \\
\mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1, \ldots, p_n\}"'] & \mathbb{F}^n
\end{tikzcd}$$

$$P(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

where $a_{ij}, b_i, c \in \mathbb{K}$.

Patarin's HFE System

$P(X)$ is

- of low total degree, D (efficient decryption).
- quadratic over $\mathbb{F}$ so that $p_i(x_1, \ldots, x_n)$ are quadratic (efficient encryption)

$$
\begin{tikzcd}
\mathbb{K} \arrow[r, "P(X)"] & \mathbb{K} \arrow[d, "\tau"] \\
\mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1, \ldots, p_n\}"] & \mathbb{F}^n
\end{tikzcd}
$$

$$P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

where $a_{ij}, b_i, c \in \mathbb{K}$.

$P(X)$ is

- of low total degree, D (efficient decryption).
- quadratic over $\mathbb{F}$ so that $p_i(x_1, \ldots, x_n)$ are quadratic (efficient encryption)

$$
\begin{tikzcd}
\mathbb{K} \arrow[r, "P(X)"] & \mathbb{K} \arrow[d, "\tau"'] \\
\mathbb{F}^n \arrow[u, "\sigma"] \arrow[r, "\{p_1, \ldots, p_n\}"] & \mathbb{F}^n
\end{tikzcd}
$$

$$P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

where $a_{ij}, b_i, c \in \mathbb{K}$.

Patarin's HFE System

$P(X)$ is

- of low total degree, D (efficient decryption).
- quadratic over $\mathbb{F}$ so that $p_i(x_1, \ldots, x_n)$ are quadratic (efficient encryption)

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{P(X)} & \mathbb{K} \\ \sigma \uparrow & & \downarrow \tau \\ \mathbb{F}^n & \xrightarrow{\{p_1, \ldots, p_n\}} & \mathbb{F}^n \end{array}$$

$$P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

where $a_{ij}, b_i, c \in \mathbb{K}$.

Outline

Systems with a unique solution

Suppose the system

$$\begin{aligned} p_1(x_1,\dots,x_n) &= 0 \\ p_2(x_1,\dots,x_n) &= 0 \\ &\vdots \\ p_n(x_1,\dots,x_n) &= 0 \end{aligned}$$

If the system has the unique solution,

$$x_1 = a_1, x_2 = a_2, \dots, x_n = a_n$$

then

$$(p_1(x_1,\dots,x_n),\dots,p_n(x_1,\dots,x_n)) = (x_1 - a_1, x_2 - a_2 \dots x_n - a_n)$$

$$x_i - a_i = \sum_{i=1}^{n} g_j(x_1,\dots,x_n) p_j(x_1,\dots,x_n)$$

So $x_i - a_i$ can be found by exhaustive search of all combinations of the form $\sum_{i=1}^{n} g_j(x_1,\dots,x_n) p_j(x_1,\dots,x_n)$ or by Gröbner basis algorithms.

Systems with a unique solution

Suppose the system

$$
\begin{aligned}
p_1(x_1, \ldots, x_n) &= 0 \\
p_2(x_1, \ldots, x_n) &= 0 \\
&\vdots \\
p_n(x_1, \ldots, x_n) &= 0
\end{aligned}
$$

If the system has the unique solution,

$$x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$$

then

$$(p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)) = (x_1 - a_1, x_2 - a_2 \ldots x_n - a_n)$$

$$x_i - a_i = \sum_{i-1}^{n} g_j(x_1, \ldots, x_n) p_j(x_1, \ldots, x_n)$$

So $x_i - a_i$ can be found by exhaustive search of all combinations of the form $\sum_{i-1}^{n} g_j(x_1, \ldots, x_n) p_j(x_1, \ldots, x_n)$ or by Gröbner basis algorithms.

Systems with a unique solution

Suppose the system

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ p_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ p_n(x_1, \ldots, x_n) &= 0 \end{aligned}$$

If the system has the unique solution,

$$x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$$

then

$$(p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)) = (x_1 - a_1, x_2 - a_2 \ldots x_n - a_n)$$

$$x_i - a_i = \sum_{i-1}^{n} g_j(x_1, \ldots, x_n) p_j(x_1, \ldots, x_n)$$

So $x_i - a_i$ can be found by exhaustive search of all combinations of the form $\sum_{i-1}^{n} g_j(x_1, \ldots, x_n) p_j(x_1, \ldots, x_n)$ or by Gröbner basis algorithms.

Let $A = \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$; set $x_i = \bar{X}_i$.

$$A_k = \{\text{elements expressible as polynomials of degree} \leq \text{k}\}$$

Let

$$I = (p_1(x_1, \ldots, x_n), \ldots, p(x_1, \ldots, x_n)) = \sum_i Ap_i(x_1, \ldots, x_n)$$

where $\deg p_i = d_i$. Note that $\dim A/I$ equals the number of solutions of the system. Set

$$J_k = \sum_i A_{k-d_i} p_i \subset A_k$$

Then

$$J_1 \subset J_2 \subset \cdots \subset J_N = I$$

When $\dim A_k - \dim J_k < q$ we can find a univariate polynomial in J_k which can be solved by univariate root-finding algorithms to find a_i.

XL algorithm

Let $A = \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$; set $x_i = \bar{X}_i$.

$$A_k = \{\text{elements expressible as polynomials of degree} \leq \text{k }\}$$

Let

$$I = (p_1(x_1, \ldots, x_n), \ldots, p(x_1, \ldots, x_n)) = \sum_i A p_i(x_1, \ldots, x_n)$$

where $\deg p_i = d_i$. Note that $\dim A/I$ equals the number of solutions of the system.

Set

$$J_k = \sum_i A_{k-d_i} p_i \subset A_k$$

Then

$$J_1 \subset J_2 \subset \cdots \subset J_N = I$$

When $\dim A_k - \dim J_k < q$ we can find a univariate polynomial in J_k which can be solved by univariate root-finding algorithms to find a_i.

XL algorithm

Let $A = \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$; set $x_i = \bar{X}_i$.

$$A_k = \{\text{elements expressible as polynomials of degree} \leq \text{k }\}$$

Let

$$I = (p_1(x_1, \ldots, x_n), \ldots, p(x_1, \ldots, x_n)) = \sum_i A p_i(x_1, \ldots, x_n)$$

where $\deg p_i = d_i$. Note that $\dim A/I$ equals the number of solutions of the system.
Set

$$J_k = \sum_i A_{k-d_i} p_i \subset A_k$$

Then

$$J_1 \subset J_2 \subset \cdots \subset J_N = I$$

When $\dim A_k - \dim J_k < q$ we can find a univariate polynomial in J_k which can be solved by univariate root-finding algorithms to find a_i.

Definition

The *operational degree* of the XL algorithm is the highest degree of polynomials that occur in the calculations before the algorithm terminates

Conjecture (or Definition (Yang-Chen-Courtois))

If there are no non-trivial relations between the f_i of degree less than or equal to k, then

$$\dim A_k - \dim J_k = [t^k]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Rationale ($m = 1$, $J_k = A_{k-d}f$): since $(1 - f^{q-1})f = f - f^q = 0$

$$0 \longrightarrow \cdots \longrightarrow A_{k-2qd} \xrightarrow{1-f^{q-1}} A_{k-(q+1)d} \xrightarrow{f} A_{k-qd} \xrightarrow{1-f^{q-1}} A_{k-d} \xrightarrow{f} A_k \longrightarrow A_k/J_k \longrightarrow 0$$

So $\dim A_k/J_k = \sum_j (\dim A_{k-jqd} - \dim A_{k-(jq+1)d})$

Definition

The *operational degree* of the XL algorithm is the highest degree of polynomials that occur in the calculations before the algorithm terminates

Conjecture (or Definition (Yang-Chen-Courtois))

If there are no non-trivial relations between the f_i of degree less than or equal to k, then

$$\dim A_k - \dim J_k = [t^k]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Rationale ($m = 1$, $J_k = A_{k-d}f$): since $(1-f^{q-1})f = f - f^q = 0$

$$0 \to \cdots \to A_{k-2qd} \xrightarrow{1-f^{q-1}} A_{k-(q+1)d} \xrightarrow{f} A_{k-qd} \xrightarrow{1-f^{q-1}} A_{k-d} \xrightarrow{f} A_k \to A_k/J_k \to 0$$

So $\dim A_k/J_k = \sum_j (\dim A_{k-jqd} - \dim A_{k-(jq+1)d})$

Operational Degree of XL algorithm

Definition

The *operational degree* of the XL algorithm is the highest degree of polynomials that occur in the calculations before the algorithm terminates

Conjecture (or Definition (Yang-Chen-Courtois))

If there are no non-trivial relations between the f_i of degree less than or equal to k, then

$$\dim A_k - \dim J_k = [t^k]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Rationale ($m=1$, $J_k = A_{k-d}f$): since $(1-f^{q-1})f = f - f^q = 0$

$$0 \to \cdots \to A_{k-2qd} \xrightarrow{1-f^{q-1}} A_{k-(q+1)d} \xrightarrow{f} A_{k-qd} \xrightarrow{1-f^{q-1}} A_{k-d} \xrightarrow{f} A_k \to A_k/J_k \to 0$$

So $\dim A_k/J_k = \sum_j (\dim A_{k-jqd} - \dim A_{k-(jq+1)d})$

Yang-Chen formula

Let

$$s_d = [t^d]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Typical behavior for a set of 20 quadratic polynomials in 20 variables over $\mathbb{F}_3$.

d	0	1	2	3	4	5	6	7	8
$\dim A_d$	1	21	231	1771	10626	53110	229810	883410	2089395
$\dim J_d$	0	0	20	420	4430	31030	161350	661030	2089394
$\dim A_d - \dim J_d$	1	21	211	1331	5776	17480	33650	18470	1
s_d	1	21	211	1331	5776	17480	33650	18470	-125740

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system $f_1, \ldots, f_m$ is at most

$$\operatorname{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right) = \min\{d \mid s_d \leq 0\}$$

Yang-Chen formula

Let

$$s_d = [t^d]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Typical behavior for a set of 20 quadratic polynomials in 20 variables over $\mathbb{F}_3$.

d	0	1	2	3	4	5	6	7	8
$\dim A_d$	1	21	231	1771	10626	53110	229810	883410	2089395
$\dim J_d$	0	0	20	420	4430	31030	161350	661030	2089394
$\dim A_d - \dim J_d$	1	21	211	1331	5776	17480	33650	18470	1
s_d	1	21	211	1331	5776	17480	33650	18470	-125740

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system $f_1, \ldots, f_m$ is at most

$$\operatorname{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right) = \min\{d \mid s_d \leq 0\}$$

Yang-Chen formula

Let

$$s_d = [t^d]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Typical behavior for a set of 20 quadratic polynomials in 20 variables over $\mathbb{F}_3$.

d	0	1	2	3	4	5	6	7	8
$\dim A_d$	1	21	231	1771	10626	53110	229810	883410	2089395
$\dim J_d$	0	0	20	420	4430	31030	161350	661030	2089394
$\dim A_d - \dim J_d$	1	21	211	1331	5776	17480	33650	18470	1
s_d	1	21	211	1331	5776	17480	33650	18470	-125740

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system $f_1, \dots, f_m$ is at most

$$\operatorname{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right) = \min\{d \mid s_d \le 0\}$$

Yang-Chen formula

Let

$$s_d = [t^d]\left(\frac{(1-t^q)^n}{(1-t)^{n+1}} \prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})} \right)$$

Typical behavior for a set of 20 quadratic polynomials in 20 variables over $\mathbb{F}_3$.

d	0	1	2	3	4	5	6	7	8
$\dim A_d$	1	21	231	1771	10626	53110	229810	883410	2089395
$\dim J_d$	0	0	20	420	4430	31030	161350	661030	2089394
$\dim A_d - \dim J_d$	1	21	211	1331	5776	17480	33650	18470	1
s_d	1	21	211	1331	5776	17480	33650	18470	-125740

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system $f_1, \ldots, f_m$ is at most

$$\operatorname{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}} \prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})} \right) = \min\{d \mid s_d \leq 0\}$$

Asymptotics of the Index

Definition

The index of a power series $\sum_i a_i t^i$, denoted $\mathrm{Ind}(\sum_i a_i t^i)$ is the first k such that $a_k \leq 0$.

Problem

Understand the behavior of

$$\mathrm{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Theorem

(The case when $q = 2$, $n = m$ and $d_1 = \cdots = d_n = 2$). Asymptotically,

$$\mathrm{Ind}\left(\frac{(1-t^2)^n}{(1-t)^{n+1}}\left(\frac{(1-t^2)}{(1-t^{2q})}\right)^n\right) \cong .09n$$

Asymptotics of the Index

Definition

The index of a power series $\sum_i a_i t^i$, denoted $\mathrm{Ind}(\sum_i a_i t^i)$ is the first k such that $a_k \leq 0$.

Problem

Understand the behavior of

$$\mathrm{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Theorem

(The case when $q=2$, $n=m$ and $d_1=\cdots=d_n=2$). Asymptotically,

$$\mathrm{Ind}\left(\frac{(1-t^2)^n}{(1-t)^{n+1}}\left(\frac{(1-t^2)}{(1-t^{2q})}\right)^n\right) \cong .09n$$

Asymptotics of the Index

Definition

The index of a power series $\sum_i a_i t^i$, denoted $\mathrm{Ind}(\sum_i a_i t^i)$ is the first k such that $a_k \leq 0$.

Problem

Understand the behavior of

$$\mathrm{Ind}\left(\frac{(1-t^q)^n}{(1-t)^{n+1}}\prod_i \frac{(1-t^{d_i})}{(1-t^{d_i q})}\right)$$

Theorem

(The case when $q=2$, $n=m$ and $d_1=\cdots=d_n=2$). Asymptotically,

$$\mathrm{Ind}\left(\frac{(1-t^2)^n}{(1-t)^{n+1}}\left(\frac{(1-t^2)}{(1-t^{2q})}\right)^n\right) \cong .09n$$

Conclusion and Applications to MPKC

Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC's like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the f_i's as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.

Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC's like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the f_i's as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.

Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC's like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the f_i's as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.

Conclusion and Applications to MPKC

Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC's like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the f_i's as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.

Outline

Definition

First Fall Degree: Lowest degree at which non-trivial "degree falls" occur.

$$\deg\left(\sum_i g_i p_i\right) < \max\{\deg(g_i) + \deg(p_i)\}$$

Trivial degree falls:

$$p_i^{q-1} p_i = p_i^q = p_i, \quad p_j p_i - p_i p_j = 0$$

Example

If $q = 2$ and $p(x_1, \ldots, x_6) = x_1x_2 + x_3x_4 + x_5x_6 + 1$ then

$$x_1x_3x_5(x_1x_2 + x_3x_4 + x_5x_6 + 1) = x_1x_2x_3x_5 + x_1x_3x_4x_5 + x_1x_3x_5x_6 + x_1x_3x_5$$

is a non-trivial degree fall.

First Fall Degree

Definition

First Fall Degree: Lowest degree at which non-trivial "degree falls" occur.

$$\deg\left(\sum_i g_i p_i\right) < \max\{\deg(g_i) + \deg(p_i)\}$$

Trivial degree falls:

$$p_i^{q-1} p_i = p_i^q = p_i, \quad p_j p_i - p_i p_j = 0$$

Example

If $q = 2$ and $p(x_1, \ldots, x_6) = x_1 x_2 + x_3 x_4 + x_5 x_6 + 1$ then

$$x_1 x_3 x_5 (x_1 x_2 + x_3 x_4 + x_5 x_6 + 1) = x_1 x_2 x_3 x_5 + x_1 x_3 x_4 x_5 + x_1 x_3 x_5 x_6 + x_1 x_3 x_5$$

is a non-trivial degree fall.

First Fall Degree of Leading Terms

Let p_i^h be the highest degree part of p_i considered as an element of the truncated polynomial ring

$$p_i^h \in \frac{\mathbb{F}[x_1, \ldots, x_n]}{\langle x_1^q, \ldots, x_n^q \rangle}$$

First fall degree of $p_1^h, \ldots, p_n^h$ is first degree at which non-trivial relations occur.

$$\deg\left(\sum_i f_i p_i^h\right) = 0$$

Trivial relations: $(p_i^h)^{q-1} p_i^h = 0, \quad p_j^h p_i^h - p_i^h p_j^h = 0$
Then

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) = D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h)$$

First Fall Degree of Leading Terms

Let p_i^h be the highest degree part of p_i considered as an element of the truncated polynomial ring

$$p_i^h \in \frac{\mathbb{F}[x_1, \ldots, x_n]}{\langle x_1^q, \ldots, x_n^q \rangle}$$

First fall degree of $p_1^h, \ldots, p_n^h$ is first degree at which non-trivial relations occur.

$$\deg\left(\sum_i f_i p_i^h\right) = 0$$

Trivial relations: $(p_i^h)^{q-1} p_i^h = 0, \quad p_j^h p_i^h - p_i^h p_j^h = 0$

Then

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) = D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h)$$

First Fall Degree of Leading Terms

Let p_i^h be the highest degree part of p_i considered as an element of the truncated polynomial ring

$$p_i^h \in \frac{\mathbb{F}[x_1, \ldots, x_n]}{\langle x_1^q, \ldots, x_n^q \rangle}$$

First fall degree of $p_1^h, \ldots, p_n^h$ is first degree at which non-trivial relations occur.

$$\deg \left(\sum_i f_i p_i^h \right) = 0$$

Trivial relations: $(p_i^h)^{q-1} p_i^h = 0, \quad p_j^h p_i^h - p_i^h p_j^h = 0$

Then

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) = D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h)$$

First-Fall Degree for HFE Systems

Theorem (Dubois-Gama)

$D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{ff}}(p_1^h, \ldots, p_j^h)$

Recall that

$$P(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

Define

$$P_0(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j \in \mathbb{K}[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q)$$

Galois theory and filtered-graded arguments yield the key result:

Theorem

$D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{ff}}(P_0)$

Theorem (Dubois-Gama)

$D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{ff}}(p_1^h, \ldots, p_j^h)$

Recall that

$$P(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

Define

$$P_0(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j \in \mathbb{K}[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q)$$

Galois theory and filtered-graded arguments yield the key result:

Theorem

$D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{ff}}(P_0)$

Theorem (Dubois-Gama)

$D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{ff}}(p_1^h, \ldots, p_j^h)$

Recall that

$$P(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

Define

$$P_0(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j \in \mathbb{K}[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q)$$

Galois theory and filtered-graded arguments yield the key result:

Theorem

$D_{\mathrm{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{ff}}(P_0)$

Bounding the First-Fall Degree for HFE Systems

Lemma

$$D_{\mathrm{ff}}\left(P_0 = \sum_{i,j} a_{ij}X_iX_j\right) \leq \frac{\mathrm{Rank}(P_0)(q-1)}{2} + 2$$

where Rank(P_0) *is the rank of the quadratic form* P_0.

For instance

$$X_1^{q-1}X_3^{q-1}\dots X_{r-1}^{q-1}(X_1X_2 + X_3X_4 + \dots + X_{r-1}X_r) = 0$$

Theorem (Ding-Hodges)

The first fall degree of the system defined by P is bounded by

$$D_{\mathrm{ff}}(p_1,\dots,p_n) \leq \frac{\mathrm{Rank}(P_0)(q-1)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1)\rfloor + 1)}{2} + 2$$

if Rank(P_0) > 1.

Bounding the First-Fall Degree for HFE Systems

Lemma

$$D_{\text{ff}}\left(P_0 = \sum_{i,j} a_{ij} X_i X_j\right) \leq \frac{\text{Rank}(P_0)(q-1)}{2} + 2$$

where $\text{Rank}(P_0)$ *is the rank of the quadratic form* P_0*.*

For instance

$$X_1^{q-1} X_3^{q-1} \ldots X_{r-1}^{q-1} (X_1 X_2 + X_3 X_4 + \ldots + X_{r-1} X_r) = 0$$

Theorem (Ding-Hodges)

The first fall degree of the system defined by P *is bounded by*

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{\text{Rank}(P_0)(q-1)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2$$

if $\text{Rank}(P_0) > 1$.

Bounding the First-Fall Degree for HFE Systems

Lemma

$$D_{\text{ff}}\left(P_0 = \sum_{i,j} a_{ij} X_i X_j\right) \leq \frac{\text{Rank}(P_0)(q-1)}{2} + 2$$

where Rank(P_0) *is the rank of the quadratic form* P_0*.*

For instance

$$X_1^{q-1} X_3^{q-1} \dots X_{r-1}^{q-1}(X_1X_2 + X_3X_4 + \dots + X_{r-1}X_r) = 0$$

Theorem (Ding-Hodges)

The first fall degree of the system defined by P *is bounded by*

$$D_{\text{ff}}(p_1, \dots, p_n) \leq \frac{\text{Rank}(P_0)(q-1)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2$$

if Rank$(P_0) > 1$*.*

Complexity of Grobner basis attack on HFE systems

For the sake of analysis of the complexity of attacks on HFE systems we usually assume that $D = O(n^{\alpha})$.

Conclusion

If we assume that the first fall degree of a system is a good indicator of the operational degree then we can conclude that the complexity of a Grobner basis attack on HFE system is quasi-polynomial.

but...

Problem

Prove that the first fall degree of a system is a good indicator of the operational degree in suitable situations.

Higher Degree Analogs of HFE

Suppose that

$$P(X) = \sum_{q^{i_1}+\cdots+q^{i_d} \le D} a_{ij} X^{q^{i_1}+\cdots+q^{i_d}} + \text{ lower degree terms}$$

and let

$$P_0(X_1, \ldots, X_n) = \sum_{q^{i_1}+\cdots+q^{i_d} \le D} a_{ij} X_{1_i} \ldots X_{i_d} \in \mathbb{K}[X_1, \ldots, X_n] / \langle X_1^q, \ldots, X_n^q \rangle$$

Lemma

$$D_{\mathrm{ff}}(P_0) \le (\mathrm{Rank}(P_0)(q-1) + d + 2)/2$$

Theorem (Hodges-Petit-Schlather)

The first fall degree of the system defined by P is bounded by

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) \le \frac{(q-1)\log_q(D-d+1) + q + d + 1}{2}$$

Higher Degree Analogs of HFE

Suppose that

$$P(X) = \sum_{q^{i_1}+\cdots+q^{i_d} \leq D} a_{ij} X^{q^{i_1}+\cdots+q^{i_d}} + \text{ lower degree terms}$$

and let

$$P_0(X_1, \ldots, X_n) = \sum_{q^{i_1}+\cdots+q^{i_d} \leq D} a_{ij} X_{1_i} \ldots X_{i_d} \in \mathbb{K}[X_1, \ldots, X_n] / \langle X_1^q, \ldots, X_n^q \rangle$$

Lemma

$$D_{\mathrm{ff}}(P_0) \leq (\mathrm{Rank}(P_0)(q-1) + d + 2)/2$$

Theorem (Hodges-Petit-Schlather)

The first fall degree of the system defined by P is bounded by

$$D_{\mathrm{ff}}(p_1, \ldots, p_n) \leq \frac{(q-1)\log_q(D-d+1) + q + d + 1}{2}$$

Suppose that

$$P(X) = \sum_{q^{i_1}+\cdots+q^{i_d}\leq D} a_{ij} X^{q^{i_1}+\cdots+q^{i_d}} + \text{ lower degree terms}$$

and let

$$P_0(X_1,\ldots,X_n) = \sum_{q^{i_1}+\cdots+q^{i_d}\leq D} a_{ij} X_{1_i}\ldots X_{i_d} \in \mathbb{K}[X_1,\ldots,X_n]/\left\langle X_1^q,\ldots,X_n^q\right\rangle$$

Lemma

$$D_{\mathrm{ff}}(P_0) \leq (\mathrm{Rank}(P_0)(q-1)+d+2)/2$$

Theorem (Hodges-Petit-Schlather)

The first fall degree of the system defined by P is bounded by

$$D_{\mathrm{ff}}(p_1,\ldots,p_n) \leq \frac{(q-1)\log_q(D-d+1)+q+d+1}{2}$$

	$q - r$					
k	1	2	3	4	5	6
1	0	0	0	0	5	5
2	0	0	0	0	15	15
3	0	0	0	0	35	35
4	0	0	0	55	70	70
5	0	0	0	121	126	126
6	0	0	0	209	210	209
7	0	0	199	325	325	320
8	0	0	400	470	470	455
9	0	0	605	640	640	605
10	0	356	811	826	826	756
11	0	690	1010	1015	1015	889
12	0	980	1189	1190	1189	980
13	315	1204	1330	1330	1325	1005
14	594	1350	1420	1420	1405	950
15	811	1416	1451	1451	1416	811
16	950	1405	1420	1420	1350	594
17	1005	1325	1330	1330	1204	315
18	980	1189	1190	1189	980	0
19	889	1015	1015	1010	690	0
20	756	826	826	811	356	0
21	605	640	640	605	0	0
22	455	470	470	400	0	0
23	320	325	325	199	0	0
24	209	210	209	0	0	0
25	126	126	121	0	0	0
26	70	70	55	0	0	0
27	35	35	0	0	0	0
28	15	15	0	0	0	0
29	5	5	0	0	0	0
30	1	0	0	0	0	0

Shifted difference of periodic sums of generalized binomial coefficients

Generalized binomial coefficients

$$(1 + z + \cdots + z^{q-1})^n = \frac{1 - z^q}{1 - z} = \sum C_q(n,k) z^k$$

Periodic or lacunary sums of generalized binomial coefficients

$$PC_q(n,k,s) = \sum_{j=-\infty}^{\infty} C_q(n, k + sj)$$

Shifted difference of periodic sums of generalized binomial coefficients

$$\Gamma_q(n,d,r,k) = PC_q(n,k,dq) - PC_q(n,k-rd,dq)$$

Generalized binomial coefficients

$$(1 + z + \cdots + z^{q-1})^n = \frac{1 - z^q}{1 - z} = \sum C_q(n,k) z^k$$

Periodic or lacunary sums of generalized binomial coefficients

$$PC_q(n,k,s) = \sum_{j=-\infty}^{\infty} C_q(n, k + sj)$$

Shifted difference of periodic sums of generalized binomial coefficients

$$\Gamma_q(n,d,r,k) = PC_q(n,k,dq) - PC_q(n,k-rd,dq)$$

Generalized binomial coefficients

$$(1+z+\cdots+z^{q-1})^n = \frac{1-z^q}{1-z} = \sum C_q(n,k)z^k$$

Periodic or lacunary sums of generalized binomial coefficients

$$PC_q(n,k,s) = \sum_{j=-\infty}^{\infty} C_q(n,k+sj)$$

Shifted difference of periodic sums of generalized binomial coefficients

$$\Gamma_q(n,d,r,k) = PC_q(n,k,dq) - PC_q(n,k-rd,dq)$$

An example of a Gamma function

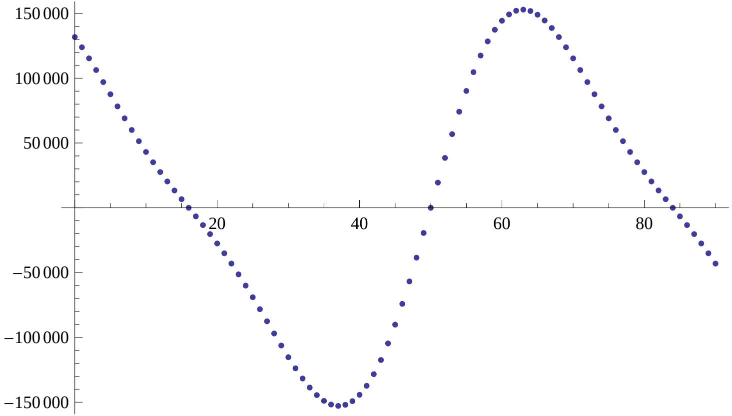

Figure: $\Gamma_{17}(6, 4, k)$

Note: $((q-1)n+d)/2 = (16.6+4)/2 = 50$

When $q = 2$, we have, for instance,

$$PC_2(n, k, 4) = \frac{2^{n-1} + 2^{n/2}\cos(\frac{\pi}{4}(n - 2k))}{2}$$

(Ramus, 1834)

If q is odd, $PC_q(n, k, r)$ is equal to

$$\frac{1}{r}\sum_{m=0}^{r-1}\left(2\sum_{j=1}^{\frac{q-1}{2}}\cos\left(\frac{m(q-2j+1)\pi}{r}\right)+1\right)^n\cos\left(\frac{m\pi((q-1)n-2k)}{r}\right)$$

(Hoggat and Alexanderson, 1976)

When $q = 2$, we have, for instance,

$$PC_2(n, k, 4) = \frac{2^{n-1} + 2^{n/2}\cos(\frac{\pi}{4}(n-2k))}{2}$$

(Ramus, 1834)

If q is odd, $PC_q(n, k, r)$ is equal to

$$\frac{1}{r}\sum_{m=0}^{r-1}\left(2\sum_{j=1}^{\frac{q-1}{2}}\cos\left(\frac{m(q-2j+1)\pi}{r}\right)+1\right)^n\cos\left(\frac{m\pi((q-1)n-2k)}{r}\right)$$

(Hoggat and Alexanderson, 1976)

Determinants with binomial coefficient entries

Problem: show that

$$\begin{vmatrix} \binom{r}{k} & \dots & \binom{r}{k+s} \\ \vdots & & \vdots \\ \binom{r+s}{k} & \dots & \binom{r+s}{k+s} \end{vmatrix}$$

is non-zero mod p if $r + s < p$.

Theorem (Zeipel, 1870's)

$$\begin{vmatrix} \binom{r}{k} & \dots & \binom{r}{k+s} \\ \vdots & & \vdots \\ \binom{r+s}{k} & \dots & \binom{r+s}{k+s} \end{vmatrix} = \frac{\binom{r}{k} \dots \binom{r+s}{k}}{\binom{k}{k} \dots \binom{k+s}{k}}$$

from: Sir Thomas Muir's "The theory of determinants in the historical order of development, Vol 3, Macmillan and Co., London, 1923"

Determinants with binomial coefficient entries

Problem: show that

$$\begin{vmatrix} \binom{r}{k} & \cdots & \binom{r}{k+s} \\ \vdots & & \vdots \\ \binom{r+s}{k} & \cdots & \binom{r+s}{k+s} \end{vmatrix}$$

is non-zero mod p if $r + s < p$.

Theorem (Zeipel, 1870's)

$$\begin{vmatrix} \binom{r}{k} & \cdots & \binom{r}{k+s} \\ \vdots & & \vdots \\ \binom{r+s}{k} & \cdots & \binom{r+s}{k+s} \end{vmatrix} = \frac{\binom{r}{k} \cdots \binom{r+s}{k}}{\binom{k}{k} \cdots \binom{k+s}{k}}$$

from: Sir Thomas Muir's "The theory of determinants in the historical order of development, Vol 3, Macmillan and Co., London, 1923"

Outline

Henceforth the base field will be $\mathbb{F}_2$.

Definition

A set $\lambda_1, \ldots, \lambda_m \in B = \mathbb{F}_2[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q)$ is semi-regular if $D_{\mathrm{ff}}(\lambda_1, \ldots, \lambda_m)$ is as large as possible.

Theorem (Bardet-Faugere-Salvy)

The set $\lambda_1, \ldots, \lambda_m$ is semi-regular if and only if

$$HS_{B/(\lambda_1,\ldots,\lambda_m)}(z) = \left[\frac{(1+z)^n}{\prod_{i=1}^m (1+z^{d_i})}\right]$$

In this case the operational degree of Grobner basis algorithms is the index of this series.

Here

$$[1 + 2t + 7t^2 + 3t^3 - 6t^4 + t^5 + \ldots] = 1 + 2t + 7t^2 + 3t^3$$

Existence of semi-regular sequences

It is widely believed that in some sense “most” sequences are semi-regular.

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

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

Existence of semi-regular sequences

It is widely believed that in some sense "most" sequences are semi-regular.

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

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