How to get rid of units?

Razvan Barbulescu
Motivation

Context
Computing discrete logs in $\mathbb{F}_{p^n}$ with $n > 1$ and small.

One wants to “turn off the Schirokauer maps”

1. when using Galois action in linear algebra (preprint theorem is correct for polys without Schirokauer maps (SMs));

2. when implementing linear algebra on GPU (current CADO for GPU is slower in presence of SMs);

3. when adapting the code to MNFS.
Joux Lercier Smart Vercauteren proposed to reduce the matrix using equations of type:

\[ \log \sigma(q) = p^\kappa \log q. \]

One can prove the equation for elements

\[ \forall x \in K, \log \sigma(x) = p^\kappa \log x. \]

The result on ideals is true only if the logs of units are zero.
Pohlig-Hellman simplification

**Logarithms modulo \( \ell \)**

1. In order to compute discrete logs in \( \mathbb{F}_{p^n} \) it is enough to implement an algorithm which computes discrete logs modulo any prime factor of \( p^n - 1 \).
2. In pairing-based cryptography, the computations are done in a subgroup of prime order \( \ell \).

**Logs in subfields when \( \ell \) divides \( \Phi_n(p) \)**

Let \( g \) be a generator of \( (\mathbb{F}_{p^n})^* \) and \( y \in (\mathbb{F}_{p^d})^* \) for some divisor \( d \) of \( n \).

\[
y^{p^d-1} = 1 \Rightarrow y^{p^n-1} = 1 \Rightarrow y^{p^n-1} = 1 \iff \log_g y \equiv 0 \pmod{\ell}.
\]
Lemma

If \( \sigma \) is an automorphism of the number field of \( f \in \mathbb{Z}[x] \) such that

- \( \sigma p = p \);  
- \( \text{Disc}(f) \not\equiv 0 \mod p \).

Then the map

\[
\overline{\sigma} : \quad k_p \quad \mapsto \quad k_p \\
\quad x \mod p \quad \mapsto \quad \sigma(x) \mod p.
\]

belongs to \( \text{Gal}(k_p) \) and \( \text{ord}(\overline{\sigma}) = \text{ord}(\sigma) \).
Logarithms of subfield elements (1/2)

\[ K \xrightarrow{\langle \sigma \rangle} \mathbb{F}_{p^k} \]

\[ K \xrightarrow{\langle \sigma \rangle} \mathbb{F}_{p^k/\text{ord}(\sigma)} \]

\[ \mathbb{Q} \xrightarrow{} \mathbb{F}_p \]
Logarithms of subfield elements (1/2)

\[ K \langle \sigma \rangle \rightarrow \mathbb{F}_{p^k}^{k/\text{ord}(\sigma)} \]

\[ x \in K^{\langle \sigma \rangle} \Rightarrow \log(x) \equiv 0 \pmod{\ell}. \]
Degree 4 family without units

**Idea**

We choose $f$ so that $\text{ord}(\sigma) = 2$ and all the units of its number field $K$ are in $K^{\langle \sigma \rangle}$.

1. signature of $K$: $(0, r)$;
2. signature of $K^{\langle \sigma \rangle}$: $(r, 0)$;

**Proposition**

Polynomials $f = x^4 + bx^3 + ax^2 + bx + 1$ are as above if and only if

1. $b^2 - 4(a - 2) > 0$;
2. and $|b| < 1 + a/2$. 
Convex subfamily
Convex subfamily
Convex subfamily

Corollary

When $|a| < 2$ and $|b| < a/2 + 1$ we can combine polys for MNFS.
Constructing pairs of polynomials without units

Algorithm

1: \( \kappa \leftarrow 100; \)
2: repeat
3: \( a \leftarrow \text{Random}(\sqrt{p}, p); \)
4: \[
\begin{pmatrix}
 u_1 \\
 v_1 \\
 u_2 \\
 v_2 
\end{pmatrix}
\leftarrow
\text{LLL}
\begin{pmatrix}
 p & 0 \\
 a & 1 
\end{pmatrix};
\]
5: until \( |u_1/v_1| < \frac{2\kappa}{2+\kappa} \) and \( |u_2/v_2| < \frac{2\kappa}{2+\kappa}. \)
6: \( a_1 \leftarrow u_1/v_1; \)
7: \( a_2 \leftarrow u_2/v_2; \)
8: \( b_1 \leftarrow a_1/\kappa; \)
9: \( b_2 \leftarrow a_2/\kappa; \)
10: return \( x^4 + b_1x^3 + a_1x^2 + b_1x + 1 \) and \( x^4 + b_2x^3 + a_2x^2 + b_2x + 1. \)

Experimental law

The termination condition occurs for \( \approx 40\% \) of values for \( a. \)
Theorem

For all positive rationals $a, b, c, d$ the polynomial

$$P(x) = (a + 3b + 3c + d)(x^2 + 4)^3 + (-3a - 6b - 3c)(x^2 + 4)^2 + (2a - 3b - 6c - d)(x^2 + 4) - 6b$$

has signature $(0, 3)$, is even and the subfield fixed by $x \mapsto -x$ has three real roots.

Proof.

$P(x) = Q(x^2 + 4)$ where $Q$ has three real roots less than 4.
Degree six family of polynomials without units

**Theorem**

For all positive rationals \( a, b, c, d \) the polynomial

\[
P(x) = (a + 3b + 3c + d)(x^2 + 4)^3 + (-3a - 6b - 3c)(x^2 + 4)^2 + (2a - 3b - 6c - d)(x^2 + 4) - 6b
\]

has signature \((0, 3)\), is even and the subfield fixed by \( x \mapsto -x \) has three real roots.

**Proof.**

\( P(x) = Q(x^2 + 4) \) where \( Q \) has three real roots less than 4.

Are there other families without units?
**Lemma**

Let $f$ be fixed polynomial with automorphism $\sigma$. For large enough prime $\ell$ we have

$$\forall \varepsilon \text{ unit}, \sigma(\varepsilon)/\varepsilon \in E^\ell \Rightarrow \sigma(\varepsilon) = \varepsilon.$$

**Theorem**

Let $n \leq 7$ be an integer, $f \in \mathbb{Z}[x]$ irreducible of degree $n$. Let $p$ be a prime and $\ell$ a factor of $\Phi_n(p)$. If $\log \rho(\varepsilon) \equiv 0 \pmod{\ell}$ for all unit $\varepsilon$, and $\ell$ is large enough, then $n = 4$ or $6$ and the number field of $f$ is CM or biquadratic real.
Characterization of polynomials “without units”

Lemma
Let $f$ be fixed polynomial with automorphism $\sigma$. For large enough prime $\ell$ we have

$$\forall \varepsilon \text{ unit}, \sigma(\varepsilon)/\varepsilon \in E^\ell \Rightarrow \sigma(\varepsilon) = \varepsilon.$$

Theorem
Let $n \leq 7$ be an integer, $f \in \mathbb{Z}[x]$ irreducible of degree $n$. Let $p$ be a prime and $\ell$ a factor of $\Phi_n(p)$. If $\log \rho(\varepsilon) \equiv 0 \pmod{\ell}$ for all unit $\varepsilon$, and $\ell$ is large enough, then $n = 4$ or 6 and the number field of $f$ is CM or biquadratic real.

Proof.

- when $n$ is prime, there are no proper subfield;
- when $n = 4$ and there are subfields $f$ is Galois, and then CM or biquadratic;
- when $n = 6$ and there are subfields then $\# \text{Gal}(f) = 6$ or 12, and then CM.
Let $E$ be the unit group of $f$.

**Vector space structure**

Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis of $E/E^\ell$.

$$(u_1, \ldots, u_r) \in \mathbb{F}_\ell^r \leftrightarrow \prod_{i=1}^{r} \varepsilon_i^u_i \in E/E^\ell.$$

**Eigenspaces**

For any eigenvalue $c \in \mathbb{F}_\ell$ of $\sigma$, we denote by $E_c$ the eigenspace of $c$:

$$E_c = \{ \epsilon \in E \mid \exists \eta \in E, \sigma(\epsilon) = \epsilon^c \eta^\ell \}.$$
Exemple of partial vanishing

- \( f = x^6 + 2x^5 - 10x^4 - 20x^3 - 5x^2 + 4x + 1; \)
- \( A = u \) root of \( \Phi_3 \) modulo \( \ell = 360187. \)
- \( \eta_i \) units depending on \( \ell \) (not on \( p \));
- \( \ell \) fixed and \( p \equiv 1039 \pmod{\ell} \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( A )</th>
<th>( E_1 )</th>
<th>( E_u )</th>
<th>( E_{u^2} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1039</td>
<td>( u )</td>
<td>0</td>
<td>( \ast )</td>
<td>( \ast )</td>
</tr>
<tr>
<td>30256747</td>
<td>( u )</td>
<td>0</td>
<td>( \ast )</td>
<td>( \ast )</td>
</tr>
<tr>
<td>46825349</td>
<td>( u )</td>
<td>0</td>
<td>( \ast )</td>
<td>( \ast )</td>
</tr>
<tr>
<td>54029089</td>
<td>( u^2 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>70597691</td>
<td>( u )</td>
<td>0</td>
<td>( \ast )</td>
<td>( \ast )</td>
</tr>
<tr>
<td>73479187</td>
<td>( u^2 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Lemma

If $A \in \mathbb{F}_\ell$ is such that $\log \rho(\sigma(x)) = A \log \rho(x) \pmod{\ell}$, then

$$\forall c \neq A, \forall \varepsilon \in E_c, \log \rho(\varepsilon) \equiv 0 \pmod{\ell}.$$
Eigenspaces

Lemma

If \( A \in \mathbb{F}_\ell \) is such that \( \log \rho(\sigma(x)) = A \log \rho(x) \pmod{\ell} \), then

\[
\forall c \neq A, \forall \varepsilon \in E_c, \log \rho(\varepsilon) \equiv 0 \pmod{\ell}.
\]

Theorem

For large enough \( \ell \), the dimension of \( E_u \) is the same for all \( u \in \mathbb{F}_\ell \) of the maximal order.

Proof.

- \( \sigma \) cancels a poly with simple roots so it is diagonal in a basis of \( \mathbb{Q}(\zeta)^r \);
- for large enough \( \ell \), the basis projects into a basis of \( \mathbb{F}_\ell^r \), so \( \dim E_\gamma = \dim E_{\gamma^i} \);
- \( \dim E_\gamma = \dim E_{\gamma^i} \) when \( \gcd(i, n) = 1 \) because automorphisms of \( \mathbb{Q}(\zeta) \) are semi-linear maps.
Odd prime degree

- totally real;
- \( \dim E_1 = 0 \) because no subfields;
- \( \dim E_u = 1 \) for all \( u \) because same dimension.

Degree 4 and 6

Depending on the signatures of \( K \) and \( K^{\langle \sigma \rangle} \) there are 16 cases.
# Degree 4 and 6 (table)

<table>
<thead>
<tr>
<th></th>
<th>$\text{deg}(K)$</th>
<th>$\text{ord}(\sigma)$</th>
<th>$\text{rk}(K)$</th>
<th>$\text{rk}(K^{\langle \sigma \rangle})$</th>
<th>$\text{dim } E_u$</th>
<th>example</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
<td>$x^4 - 5x^2 + 2$</td>
</tr>
<tr>
<td>ii</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>$x^4 - 5x^2 - 2$</td>
</tr>
<tr>
<td>iii</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>$x^4 - x^2 + 2$</td>
</tr>
<tr>
<td>iv</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td>$x^4 + 5x^2 + 2$</td>
</tr>
<tr>
<td>v</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td></td>
<td>$x^4 + x^3 - 6x^2 - x + 1$</td>
</tr>
<tr>
<td>vi</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
<td>$x^4 + x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>vii</td>
<td>6</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td></td>
<td>$x^6 - 6x^4 + 9x^2 - 3$</td>
</tr>
<tr>
<td>viii</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td></td>
<td>$x^6 - 3x^2 + 1$</td>
</tr>
<tr>
<td>ix</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
<td>$x^6 + 3x^2 - 1$</td>
</tr>
<tr>
<td>x</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
<td>$x^6 - 3x^2 - 1$</td>
</tr>
<tr>
<td>xi</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>$x^6 + 3x^2 + 1$</td>
</tr>
<tr>
<td>xii</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td></td>
<td>$x^6 + 6x^4 + 8x^2 + 1$</td>
</tr>
<tr>
<td>xiii</td>
<td>6</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>$x^6 - 8x^4 + 6x^3 + 7x^2 - 6x + 1$</td>
</tr>
<tr>
<td>xiv</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td></td>
<td>$x^6 - 5x^4 + 10x^2 - 6x + 1$</td>
</tr>
<tr>
<td>xv</td>
<td>6</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td></td>
<td>$x^6 + 2x^5 - 10x^4 - 20x^3 - 5x^2 + 4x + 1$</td>
</tr>
<tr>
<td>xvi</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td></td>
<td>$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$</td>
</tr>
</tbody>
</table>