Smallest Reduction Matrix of Binary Quadratic Forms
And Cryptographic Applications

Aurore Bernard - XLIM, Limoges, France

Joint work with Nicolas Gama - EPFL, Switzerland

9th Algorithmic Number Theory Symposium

July 19-23, 2010
Overview

Main result: minimize the size of the reduction matrices and prove an optimal upper bound on its size.

Cryptanalysis application: fully prove the factorization of the NICE modulus which is a particular case of $pq^2$ integers.

Outline:

- Introduction
  - Expected size of the smallest reduction matrix
  - Reduction algorithm
  - NICE cryptosystem
  - Factorization of the NICE modulus

Conclusion
A form is a homogeneous polynomial of degree two in 2 variables:

\[ f(x, y) = ax^2 + bxy + cy^2, \text{ with } (a, b, c) \in \mathbb{Z}^3, \]

its discriminant is \( \Delta = b^2 - 4ac \).

We distinguish two kinds of forms depending upon the sign of the discriminant: the imaginary \( (\Delta < 0) \) forms and the real \( (\Delta > 0) \) forms.

Example of the surface created from both forms:

In red: the surface created from an imaginary form
In gray: the plane \( z=0 \)

In red: the surface created from a real form.
In gray: the plane \( z=0 \)

In this talk we concentrate on the real forms.
Natural action: the change of basis of the lattice $\mathbb{Z}^2$

A form $f$ written in the canonical basis:

$$f(x, y) = 3x^2 + xy - y^2$$

The same form written in the basis $(\vec{u}_1, \vec{u}_2)$:

$$f(\vec{u}_1 x + \vec{u}_2 y) = 29x^2 + 77xy + 51y^2$$

The polar representation of a form $(a, b, c)$ in the basis $(\vec{u}_1, \vec{u}_2)$ of the lattice $\mathbb{Z}^2$ is:

$$\mathcal{B}^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \mathcal{B}$$

with $\mathcal{B}$ the change of basis matrix.
Natural equivalence relation between the forms of same discriminant

A form:
\[ f(x, y) = 3x^2 + xy - y^2 \]

An equivalent form:
\[ g(x, y) = 29x^2 + 77xy + 51y^2 \]

A transition matrix from \( f \) to \( g \):
\[
\begin{pmatrix}
3 & 4 \\
2 & 3
\end{pmatrix}
\]

The two forms \( f \) and \( g \) are **equivalents** if there is exists a basis of the lattice \( \mathbb{Z}^2 \) such as \( g \) is the form \( f \) written in this basis.

The change of basis matrix is called the **transition matrix** from \( f \) to \( g \).

It is an equivalence relation: reflexive, symmetric, transitive.
Expected size of the smallest reduction matrix
Global problem of the smallest reduction matrix

Find the smallest basis in which the polar representation of $f$ is "small" (i.e. coefficients of size $\approx \sqrt{\Delta}$).

Problem of the good basis

Find the smallest basis $(\vec{u}_1, \vec{u}_2)$ such as $f(\vec{u}_1) \cdot f(\vec{u}_2) < 0$.

Example of equivalent forms, in blue their negative points:

Far from being a reduced form
$5277x^2 + 2675xy + 339y^2$

almost a reduced form
$29x^2 + 77xy + 51y^2$

Reduced form
$3x^2 + xy - y^2$
Let $f = (a, b, c)$ be a form with positive $a$ and $c$.

In order to find the good basis, we just need to find the smallest $\vec{u}_1 \in \mathbb{Z}^2$ such as $f(\vec{u}_1) < 0$.

The second basis vector $\vec{u}_2$ is determined by Bézout coefficients on $\vec{u}_1$.

The expected size of the smallest reduction matrix is the size of $\vec{u}_1$.

Previous forms with view from above, we want find negative points:
Specific disposition of the negative points of a form

According to the factorization of a form: $f(x, y) = a(x - y\zeta^{-})(x - y\zeta^{+})$

$f < 0$ when $(x, y)$ are between the lines $x = y\zeta^{-}$ and $x = y\zeta^{+}$.
We zoom on an almost reduced form.

We find $\vec{u}_1 \in \mathbb{Z}^2$ such as $f(\vec{u}_1) < 0$.

1) Trivial approach to find a negative point of $f$

For $x = 1$: $f < 0$ on the interval of size $\sqrt{\Delta}/a$.

According to Thales:
for $x = \lceil a/\sqrt{\Delta} \rceil$, $f < 0$ on interval of size $> 1$.

We get an integer $y$ such as $f(x, y) < 0$.

The expected size of $\vec{u}_1$ is $O \left( a/\sqrt{\Delta} \right)$. 
2) Advanced approach to find a negative point of $f$

The points where $f$ has the greater chance to be negative are very close to the line $x = \left(-\frac{b}{2a}\right)y$ (in gray) with an error of $\sqrt{\Delta}/2a$.

$x/y$ is an approximation of rational $-b/2a$ with an error of $\sqrt{\Delta}/2a$.

We compute $x/y$ from a Padé approximation, which gives an error of $1/y^2$.

And since we expect $1/y^2 < \sqrt{\Delta}/2a$, then $y$ is of expected size $O\left(\sqrt{\frac{a}{\sqrt{\Delta}}}\right)$. 
Form reduction algorithm
Let $f$ be a form, we only focus on the parabola $f(x, 1)$. We note $\zeta^-$ its smallest root and $\zeta^+$ its largest one.

All the following can be expressed using these roots.

A form is **reduced** when:

1) its roots are of opposite signs,

2) one of them has absolute value $< 1$ and the other has absolute value $> 1$. 
Problem of the reduced form

Let $f$ be a given form.
Find a transition matrix from $f$ to a reduced form.

### Integer isometries:

<table>
<thead>
<tr>
<th></th>
<th>Matrix</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E</strong>xchange</td>
<td>$\begin{pmatrix} 0 &amp; 1 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>inverts the roots</td>
</tr>
<tr>
<td><strong>S</strong>ymmetry</td>
<td>$\begin{pmatrix} 1 &amp; 0 \ 0 &amp; -1 \end{pmatrix}$</td>
<td>negates the roots</td>
</tr>
</tbody>
</table>

### Normalizations:

| $T^-$ | $\begin{pmatrix} 1 & \lfloor \zeta^- \rfloor \\ 0 & 1 \end{pmatrix}$ | brings $\zeta^- \in ] - 1; 0[$ |
| $T^+$ | $\begin{pmatrix} 1 & \lceil \zeta^+ \rceil \\ 0 & 1 \end{pmatrix}$ | brings $\zeta^+ \in ] 0; 1[$ |

The action of $E$, $S$, $T^-$, $T^+$ on the roots is a homography.
Let us recall the definition of a reduced form.

A form is reduced when:
its roots are of opposite signs,
one of them has to be of absolute value <1
and the other has to be of absolute value >1.

The last step: when there are at least 2 integers between the roots
$T^-$ or $T^+$ gives an equivalent reduced form.

The main loop: while there are less than 2 integers between the roots
$T^E(S)$ will increase the distance between the roots.
Different algorithms according to the choice of the normalization $T^-$ or $T^+$:

While there are not at least 2 integers between the roots

The last step

- **Largest** (Gauss initial): exponential

- **Rounding** of the average of the roots (Gauss-Lagarias):
  - the least number of iterations,
  - but the last steps doesn’t control the size of the reduction matrix

- **Shortest**: quadratic, smallest reduction matrix
Our results

### Smallest Reduction Matrix Theorem

Let $f = (a, b, c)$ be a normalized form and its smallest reduction matrix $M = \begin{pmatrix} u & s \\ v & t \end{pmatrix}$:

1) $\|M\|_\infty \leq 4 \sqrt{\left| \frac{a}{f(u, v)} \right|}$

2) $|us|^{1/2} \leq |vt|^{1/2} \leq \sqrt{21} \sqrt{\frac{|a|}{\sqrt{\Delta}}}$

These bounds correspond to the advanced approach to determine the expected size of the smallest reduction matrix.

Using Gauss-Lagarias algorithm:
- reduction matrices can be $\sqrt{\Delta}$ times larger
- best bounds known correspond to the trivial approach
<table>
<thead>
<tr>
<th>Introduction</th>
<th>Expected size</th>
<th>Reduction algorithm</th>
<th>NICE</th>
<th>Factorization</th>
<th>Conclusion</th>
</tr>
</thead>
</table>

NICE cryptosystem
For each form $f$
- there is a finite number of reduced forms equivalent to $f$,
- they form a (reduced) cycle, which can be enumerated without memory.

Reduction:
Shortest Normalization + ES

Direct Neighbor on reduced cycle:
Largest Normalization + ES

Equivalence test of two forms $f$ and $g$:
1: $\tilde{f} \leftarrow \text{Reduction}(f)$
2: $\tilde{g} \leftarrow \text{Reduction}(g)$
3: Enumerate the cycle of $\tilde{f}$ until either $\tilde{f}$ or $\tilde{g}$ is found.
In practice: can we enumerate all the cycle?

Number of reduced forms per cycle:

General:
\[ \Omega(\sqrt{\Delta}) \]

\( \Delta = p \) a Schinzel prime:
\[ \Theta(\log(p)) \]

\( \Delta = pq^2 \) with \( p \) a Schinzel prime:
\[ \Theta(q \log(p)) \]
Two kinds of forms according to their discriminant: $\mathcal{F}_p$ and $\mathcal{F}_N= pq^2$.

Each form of $\mathcal{F}_N$:

1) is equivalent by a good translation to a form $(a, qb, q^2c)$,

2) its Lift is $(a, b, c) \in \mathcal{F}_p$.

Two equivalent forms also have equivalent Lift.
Two particular cases:

1) \(|a| < \sqrt{p}/2\): \((a, b, c) \in \mathbb{F}_N\) is reduced, 
   \(\text{Lift}(f) = (a, b, c)\) is reduced.
Two particular cases:

1) \(|a| < \sqrt{p}/2\): \((a, b, c) \in \mathcal{F}_N\) is reduced, 
   \(\text{Lift}(f) = (a, b, c)\) is reduced.

2) \(p\) a Schinzel prime and \(a\) satisfies some pattern.

Which implies that:

- Given an equivalent form \(f\) and the factor \(q\), then it’s easy to find \(a\).
- It was assumed that, given just \(f\) and \(N\), then it’s impossible to find \(a\).
Key Generation: the secret keys are a Schinzel prime $p$ and a prime $q$; the public key is $N = pq^2$

Encryption:
- pad $m$ into a prime $a < \sqrt{p}/2$ satisfying a pattern
- create a form $(a, b, c) \in \mathcal{F}_N$
- output a random form $f$ on the cycle of $(a, b, c)$

Decryption:
- enumerate the cycle of $\text{Lift}(f)$
- recover $a$, then $m$
<table>
<thead>
<tr>
<th>Introduction</th>
<th>Expected size</th>
<th>Reduction algorithm</th>
<th>NICE</th>
<th>Factorization</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack on NICE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Attack**: factorize the NICE modulus
We focus on $1_N$ which contains $(1, \ldots) \in \mathcal{F}_N = pq^2$.

We know that there is a large number of forms $(q^2, \ldots)$ equivalent to $(1, \ldots)$, and they form the $q$-belt.

Note that $(1, \ldots)$ and $1_N$ are public since $N$ is the public key of the NICE cryptosystem.
The process of the attack is to enumerate the right neighbor of \((1, \ldots, )\), and to try to backtrack to one of the \(q\)-belt, then we recover the factorization of \(N\).

Our Results:

1) We can backtrack ALL the reduction of the \(q\)-belt.

2) The closest that it backtracks is at a polynomial DISTANCE from \((1, \ldots, )\)
The distance between forms is the size of the smallest transition matrix.

- satisfies the triangle inequality

The shortest path between 2 reduced forms is along the cycle.

Any transition matrix smaller than half the cycle is the smallest.
$q$-Recover Theorem

Given $(a, b, c)$ and $N = pq^2$, a variant of Coppersmith’s algorithm solves

$$au^2 + buv + cv^2 = 0 \pmod{q^2}$$

in $(u, v, q)$ for $|uv| \leq N^{2/9}$

in polynomial time.

It’s means that: from any form "close" to $(t \cdot q^2, .., .)$ for any integer $t$, we obtain $q^2$ by applying our variant of Coppersmith’s algorithm.

We represent the forms "close to" by the green zone.
An **attackable form** is a form which is "close" to \((q^2, \ldots)\) (in the green zone).

The \(q\)-recover Theorem prove that these forms give us the factorization of \(N\).

We prove that we can recover \(q\) from an attackable forms which is on the cycle.

There are several possible meaning of "close" according to variant\(^1\) of Coppersmith’s algorithm used.

\(^1\) Factoring \(pq^2\) with Quadratic Forms: NICE Cryptanalyses- Castagnos, Joux, Laguillaumie, Nguyen - Asiacrypt 2009
The previous attack: classical reduction and previous attackable forms.

There is no proof of the intersection with $1_N$, then we can not prove that it recovers $q$. 

"..."
The previous attack with the Smallest Reduction Matrix Theorem.

Sometimes there is an intersection with \( \mathbb{1}_N \), but there is no proof that it is always true. The first intersection can be exponentially far from \((1, \ldots, 1)\).
The attack with the **Smallest Reduction Matrix Theorem** and the **$q$-Recover Theorem**.

There is always an intersection with $\mathbb{1}_N$, therefore it proves that $q$ can always be recovered from an attackable form.
At last, we still need to prove that the first attackable form is at a polynomial distance from \((1, \ldots)\).
The transition matrices from $(1, \ldots) \in \mathcal{F}_N$ to the $q$-belt:

Lift $(1, \ldots) \in \mathcal{F}_N$, turn around the $(1, \ldots) \in \mathcal{F}_p$, and Unlift.
A Lift involves a transition matrix of determinant $1/q$, then it is not an integer operation on the transition matrices.

An Unlift is not exactly the inverse of Lift: the $(1,..,.) \in \mathbb{F}_p$ has many preimages by the Lift, which are the $(1,..,.) \in \mathbb{F}_N$ and the q-belt.
If one tries to make a path which starts by a lift, and ends by some unlift operation, only one of the preimages will yield an integer transition matrix.

If one lifts from \((1, \ldots) \in \mathcal{F}_N\) to \((1, \ldots) \in \mathcal{F}_p\), the only integer transition matrix we can get by unlifting will bring us back to \((1, \ldots) \in \mathcal{F}_N\), which is totally useless.
However, if we lift from $(1, \ldots) \in \mathcal{F}_N$, and turn around the cycle of $p$, then we can prove that Unlifting will necessarily bring us to another preimage, which starts by $q^2$. This is exactly what we need!
The fact that $p$ is a Schinzel prime renders this path polynomial, then it makes the attack practical.
**Gauss Algorithm**

- obtains the smallest reduction matrix
- (very) tight bounds on the reduction matrix

**NICE Cryptosystem**

- NICE is provably and practically broken
Thanks for your attention