On the extremality of an 80-dimensional lattice

Damien Stehlé and Mark Watkins

LIP – CNRS/ENSL/U. Lyon/INRIA/UCBL

ANTS-IX, July 2010

The result

THEOREM

One of the even unimodular lattices associated to the length 80 extended (binary) quadratic residue code is extremal:
the minimal non-zero norm is 8. We have $\mathbf{SL}_2(\mathbf{F}_{79}) \subseteq \mathbf{Aut}(L)$.

The result

THEOREM

One of the even unimodular lattices associated to the length 80 extended (binary) quadratic residue code is extremal: the minimal non-zero norm is 8. We have $\mathbf{SL}_2(\mathbf{F}_{79}) \subseteq \mathbf{Aut}(L)$.

- L and its link to coding theory (via cyclotomy) was codified by Schulze-Pillot, who could not find any norm 6 vector.
- If $n > 80$, a lattice related to QR codes cannot be extremal. (sqrt bound on minimum versus linear growth requirement).
- No extremal lattice known for $n = 72$ (or $n > 80$).
- Bachoc and Nebe previously found two other extremal lattices with $n = 80$, via quaternionic coding theory.
- The known part of our $\mathbf{Aut}(L)$ is smaller: $8.3 \cdot 10^6 > 4.9 \cdot 10^5$.

The techniques

THEOREM

One of the even unimodular lattices associated to the length 80 extended (binary) quadratic residue code is extremal: the minimal non-zero norm is 8. We have $\mathbf{SL}_2(\mathbf{F}_{79}) \subseteq \mathbf{Aut}(L)$.

The techniques

THEOREM

One of the even unimodular lattices associated to the length 80 extended (binary) quadratic residue code is extremal: the minimal non-zero norm is 8. We have $\mathbf{SL}_2(\mathbf{F}_{79}) \subseteq \mathbf{Aut}(L)$.

- We show no norm 6 by finding **all** norm 10 vectors (!).
- This is valid, using the Θ-series positivity.
- In the short lattice vector enumeration, we use tree pruning.
- We also use nice **Aut** action (as doubly transitive signed permutations), derived in part by Abel, Elkies and Kominers.

The techniques

THEOREM

One of the even unimodular lattices associated to the length 80 extended (binary) quadratic residue code is extremal: the minimal non-zero norm is 8. We have $\mathbf{SL}_2(\mathbf{F}_{79}) \subseteq \mathbf{Aut}(L)$.

- We show no norm 6 by finding **all** norm 10 vectors (!).
- This is valid, using the Θ-series positivity.
- In the short lattice vector enumeration, we use tree pruning.
- We also use nice **Aut** action (as doubly transitive signed permutations), derived in part by Abel, Elkies and Kominers.

The enumeration part is heuristic, but we still get a proved result.

Plan

1- **Reminders.**
2- Overview of the strategy.
3- Lattice enumeration.

Lattices

Lattice $\equiv$ additive subgroup of $\mathbb{Z}^n$

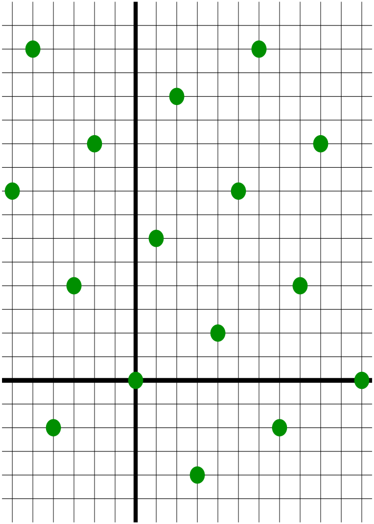
$\equiv \quad \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

First minimum:
$\lambda = \min(\|\mathbf{b}\|^2 : \mathbf{b} \in L \setminus \mathbf{0})$.

Lattice volume:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis.

Unimodular lattice: $|\det L| = 1$.
Even lattice: $\|\mathbf{b}\|^2$ even for all $\mathbf{b} \in L$.

Famous even unimod. lattices: E_8, L_{24}.



Lattices

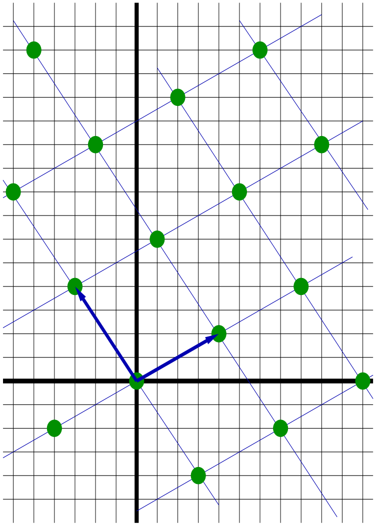
Lattice $\equiv$ additive subgroup of $\mathbb{Z}^n$
$\equiv \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

First minimum:
$\lambda = \min(\|\mathbf{b}\|^2 : \mathbf{b} \in L \setminus \mathbf{0})$.

Lattice volume:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis.

Unimodular lattice: $|\det L| = 1$.
Even lattice: $\|\mathbf{b}\|^2$ even for all $\mathbf{b} \in L$.

Famous even unimod. lattices: E_8, L_{24}.



Lattices

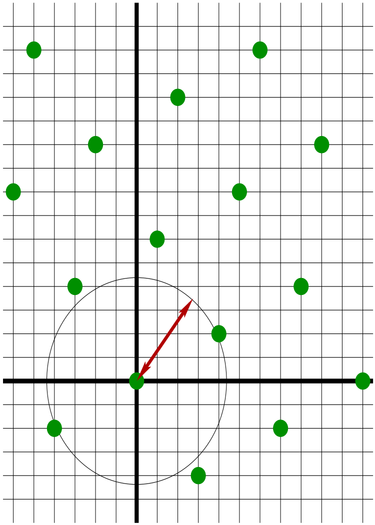
Lattice $\equiv$ additive subgroup of $\mathbb{Z}^n$
$\equiv \{\sum_{i \le n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

First minimum:
$\lambda = \min(\|\mathbf{b}\|^2 : \mathbf{b} \in L \setminus \mathbf{0})$.

Lattice volume:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis.

Unimodular lattice: $|\det L| = 1$.
Even lattice: $\|\mathbf{b}\|^2$ even for all $\mathbf{b} \in L$.

Famous even unimod. lattices: E_8, L_{24}.



Lattices

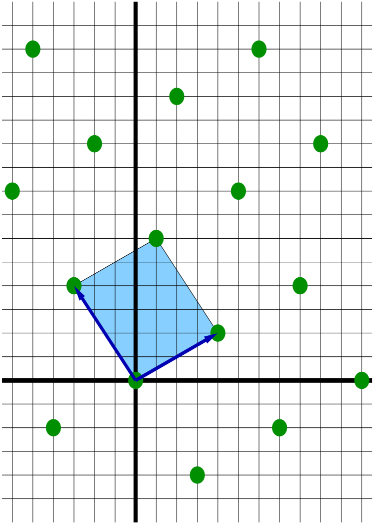
Lattice $\equiv$ additive subgroup of $\mathbb{Z}^n$
$\equiv \{\sum_{i\leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

First minimum:
$\lambda = \min(\|\mathbf{b}\|^2 : \mathbf{b} \in L \setminus \mathbf{0})$.

Lattice volume:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis.

Unimodular lattice: $|\det L| = 1$.
Even lattice: $\|\mathbf{b}\|^2$ even for all $\mathbf{b} \in L$.

Famous even unimod. lattices: E_8, L_{24}.



Lattices

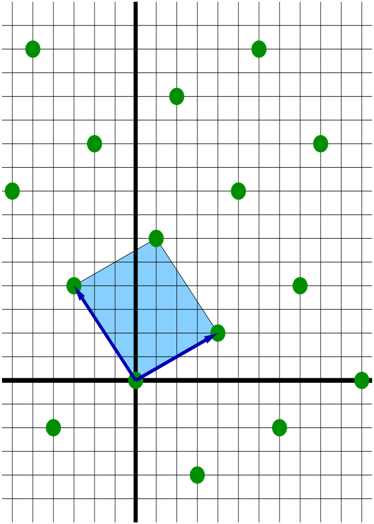
Lattice $\equiv$ additive subgroup of $\mathbb{Z}^n$
$\equiv \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$

First minimum:
$\lambda = \min(\|\mathbf{b}\|^2 : \mathbf{b} \in L \setminus \mathbf{0})$.

Lattice volume:
$\det L = |\det(\mathbf{b}_i)_i|$, for any basis.

Unimodular lattice: $|\det L| = 1$.
Even lattice: $\|\mathbf{b}\|^2$ even for all $\mathbf{b} \in L$.

Famous even unimod. lattices: E_8, L_{24}.



Theta series

- Theta-series: $\Theta(L) = \sum_{\mathbf{b} \in L} q^{\|\mathbf{b}\|^2/2}$ (non-negative coeffs).

If L is an even unimodular lattice L of dimension 8ℓ,
then $\Theta(L)$ is a modular form of weight 4ℓ.

- The set of modular forms of weight 4ℓ is a vector space of dimension $d = 1 + \lfloor 8\ell/24 \rfloor$.
- A triangular basis for this vector space looks like

$$\begin{array}{lclcccc} f_0 & = & 1+ & & & c_{d,0}\, q^d & + \ldots \\ f_1 & = & & q+ & & c_{d,1}\, q^d & + \ldots \\ & & & \ldots & & & \\ f_{d-1} & = & & & q^{d-1}+ & c_{d,d-1}\, q^d & + \ldots \end{array}$$

- An even unimodular L is said **extremal** if $\Theta(L) = f_0$.

General comments about extremality

- For large enough n, f_0 has negative coeffs.
  $\Rightarrow$ The total number of extremal lattices is bounded:

$$n \leq 163\,264 \quad \& \quad \text{genus theory in fixed } n.$$

- If n not a multiple of 8, minus signs abound, so no extremality is possible (for our definition).

Number of known extremal lattices:

8	16	24	32	40	48	56	64	72	80
1	2	1	$\geq 10^7$	$\geq 10^{51}$	3	3	1	0	2(+1)
E_8	$E_8 \oplus E_8$, D_{16}^+	L_{24}	mass formula						

Plan

1- Reminders.

2- **Overview of the strategy.**

3- Lattice enumeration.

Plan to show extremality

Case of 80-dimensional lattices (weight 40 modular forms):

$$
\begin{aligned}
f_0 &= 1 + 1250172000\, q^4 + 7541401190400\, q^5 + O(q^6)\\
f_1 &= q + 19291168\, q^4 + 37956369150\, q^5 + O(q^6)\\
f_2 &= q^2 + 156024\, q^4 + 57085952\, q^5 + O(q^6)\\
f_3 &= q^3 + 168\, q^4 - 12636\, q^5 + O(q^6)
\end{aligned}
$$

- We have $\Theta(L) = f_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$ for integers $a_i \geq 0$.
- L has no vector of norm ≤ 4 (via a coding theory analogy):

$$\Rightarrow \quad a_1 = a_2 = 0.$$

- Find $\approx 7.5 \cdot 10^{12}$ vectors of norm 10.
  Positivity gives $a_3 = 0$, due to the minus sign on "$12636\, q^5$".
- We use heuristics & automorphisms to get norm 10 vectors.

Searching vectors of norm 10 rather than norm 6???

- We would need to **provably exhaust** all norm 6 vectors.
- We **heuristically** find a **tiny** subset of the norm 10 vectors.
- We estimate the speed-up to be around 1000.

Principle: Apply **Aut**(L) to reduce search space.

Remark: This strategy could be used for $n = 72$ (with $10 \to 8$) and for $n = 88$ (with $10 \to 12$).

Construction of our lattice L

- The construction of L and the methods used to accelerate the finding of short vectors are independent.
- But finding a canonical representative of the orbit class of a vector (under **Aut**) requires some knowledge of the group action on L.
- Elkies modified a construction of Gross to get five 80-dim lattices, in correspondence with the class group of $\mathbf{Q}(\sqrt{-79})$. Each can be given in a basis s.t.
  - All coords have the same parity,
  - The square-sum of the coords is 16x the vector norm.
- This yields the same lattices as Schulze-Pillot's, only one of which is a candidate for extremality: L.

Apply **Aut**(L) to reduce search space

- The (known) automorphisms have a 'nice' action on Elkies' basis: doubly transitive signed permutations on coords.
  $\Rightarrow$ Finding canonical representatives of orbit classes is easy.
- Finding $\approx 7.5 \cdot 10^{12}$ vectors of norm 10 is reduced by a factor
  $$\sim \#\mathbf{SL}_2(\mathbf{F}_{79}) \approx 4.9 \cdot 10^5.$$

We first eliminate vectors with non-trivial stabilisers:

- Take $g \in \mathbf{Aut}(L)$ of nontrivial conjugacy class, and find all short vectors in lattices $\mathrm{Ker}(g - I)$ (dim ≤ 28).
- We are left to find $N \approx 1.5 \cdot 10^7$ norm 10 orbits.
- Via coupon-collecting analysis, we expect to need $\sum_{k \leq N} \frac{N}{k} \approx 2.5 \cdot 10^8$ "random" norm 10 vectors.

Plan

1- Reminders.

2- Overview of the strategy.

3- **Lattice enumeration.**

The Kannan-Fincke-Pohst algorithm

Let $(\mathbf{b}_i)$ be a basis of L. Goal: $\|\sum_i x_i \mathbf{b}_i\|^2 \leq 10$ with $x_i \in \mathbb{Z}$.

- Gram-Schmidt orthogonalisation: $\mathbf{b}_i^\star = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^\star$.
- Shifts: $y_i := x_i + \sum_{j>i} \mu_{j,i} x_j$.

$\Rightarrow$ New goal: $\sum_i y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

KFP algorithm:

- Try all y_d s.t. $y_d^2 \|\mathbf{b}_d^\star\|^2 \leq 10$.
- Try all (y_{d-1}, y_d) s.t. $\sum_{i \geq d-1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

$\vdots$

- Try all $(y_2, \ldots, y_d)$ s.t. $\sum_{i \geq 2} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.
- Try all $(y_1, \ldots, y_d)$ s.t. $\sum_{i \geq 1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

The Kannan-Fincke-Pohst algorithm

Let $(\mathbf{b}_i)$ be a basis of L. Goal: $\|\sum_i x_i \mathbf{b}_i\|^2 \leq 10$ with $x_i \in \mathbb{Z}$.

- Gram-Schmidt orthogonalisation: $\mathbf{b}_i^\star = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^\star$.
- Shifts: $y_i := x_i + \sum_{j>i} \mu_{j,i} x_j$.

$\Rightarrow$ New goal: $\sum_i y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

KFP algorithm:

- Try all y_d s.t. $y_d^2 \|\mathbf{b}_d^\star\|^2 \leq 10$.
- Try all (y_{d-1}, y_d) s.t. $\sum_{i \geq d-1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

$\vdots$

- Try all $(y_2, \ldots, y_d)$ s.t. $\sum_{i \geq 2} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.
- Try all $(y_1, \ldots, y_d)$ s.t. $\sum_{i \geq 1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

Pruning the KFP tree

Principle: Don't waste all the norm on large i!

KFP algorithm:

- Try all y_d s.t. $y_d^2 \|\mathbf{b}_d^\star\|^2 \leq 10.$
- Try all (y_{d-1}, y_d) s.t. $\sum_{i \geq d-1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10.$

$\vdots$

- Try all $(y_2, \ldots, y_d)$ s.t. $\sum_{i \geq 2} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10.$
- Try all $(y_1, \ldots, y_d)$ s.t. $\sum_{i \geq 1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10.$

Used $P_j = 1 - \frac{j-1}{100}$, which seemed good in practice.

MAGMA traverses this KFP tree at $\approx$ 7.5 million nodes/second.

Pruning the KFP tree

Principle: Don't waste all the norm on large i!

KFP algorithm:

- Try all y_d s.t. $y_d^2 \|\mathbf{b}_d^\star\|^2 \leq 10$.
- Try all (y_{d-1}, y_d) s.t. $\sum_{i \geq d-1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

$\vdots$

- Try all $(y_2, \ldots, y_d)$ s.t. $\sum_{i \geq 2} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.
- Try all $(y_1, \ldots, y_d)$ s.t. $\sum_{i \geq 1} y_i^2 \|\mathbf{b}_i^\star\|^2 \leq 10$.

Used $P_j = 1 - \frac{j-1}{100}$, which seemed good in practice.

MAGMA traverses this KFP tree at $\approx$ 7.5 million nodes/second.

Pruning the KFP tree

Principle: Don't waste all the norm on large i!

Pruned KFP algorithm:

- Try all y_d s.t. $y_d^2\|\mathbf{b}_d^\star\|^2 \leq P_d \cdot 10.$
- Try all (y_{d-1}, y_d) s.t. $\sum_{i\geq d-1} y_i^2\|\mathbf{b}_i^\star\|^2 \leq P_{d-1} \cdot 10.$

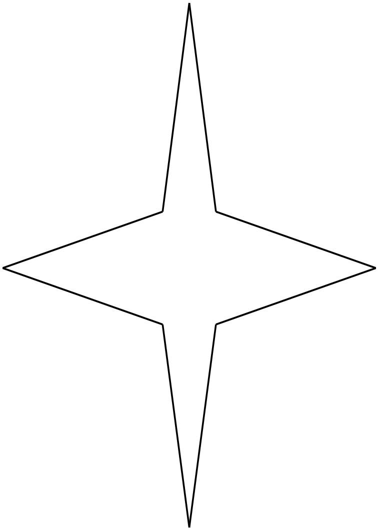
$\vdots$

- Try all $(y_2, \ldots, y_d)$ s.t. $\sum_{i\geq 2} y_i^2\|\mathbf{b}_i^\star\|^2 \leq P_2 \cdot 10.$
- Try all $(y_1, \ldots, y_d)$ s.t. $\sum_{i\geq 1} y_i^2\|\mathbf{b}_i^\star\|^2 \leq P_1 \cdot 10.$

Used $P_j = 1 - \frac{j-1}{100}$, which seemed good in practice.

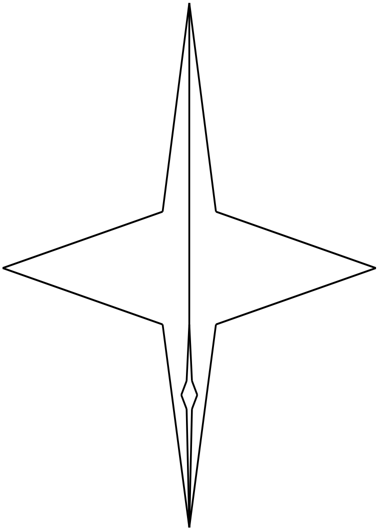
MAGMA traverses this KFP tree at $\approx$ 7.5 million nodes/second.

Refreshing the basis



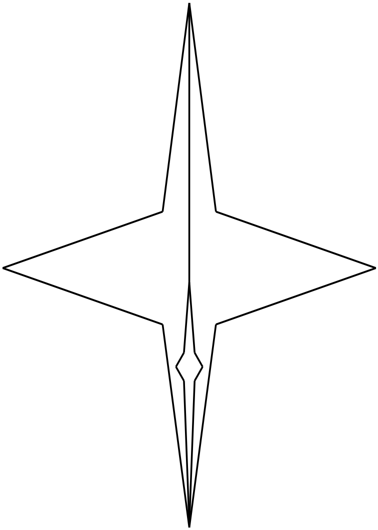
- Schnorr-Euchner tree traversal.
- Random basis change every 10^5 vecs (30 mins) $\Rightarrow$ trivial parallelisation.
- $\sim$300,000 nodes per vector found.
- Can heuristically analyze the miss rate and subtrees sizes via volumes of truncated hyperspheres.
- Resembles the "extreme pruning" from [Gama et al, Eurocrypt'10].

Refreshing the basis



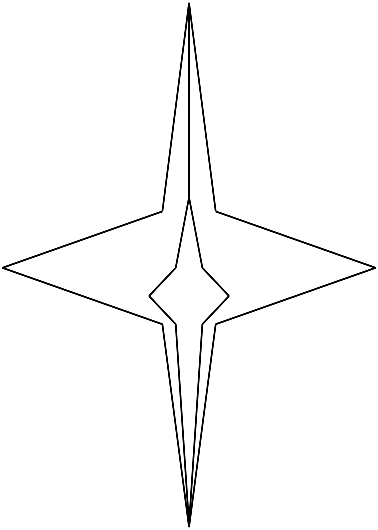
- Schnorr-Euchner tree traversal.
- Random basis change every 10^5 vecs (30 mins) $\Rightarrow$ trivial parallelisation.
- $\sim$300,000 nodes per vector found.
- Can heuristically analyze the miss rate and subtrees sizes via volumes of truncated hyperspheres.
- Resembles the "extreme pruning" from [Gama et al, Eurocrypt'10].

Refreshing the basis



- Schnorr-Euchner tree traversal.
- Random basis change every 10^5 vecs (30 mins) $\Rightarrow$ trivial parallelisation.
- $\sim$300,000 nodes per vector found.
- Can heuristically analyze the miss rate and subtrees sizes via volumes of truncated hyperspheres.
- Resembles the "extreme pruning" from [Gama et al, Eurocrypt'10].

Refreshing the basis



- Schnorr-Euchner tree traversal.
- Random basis change every 10^5 vecs (30 mins) $\Rightarrow$ trivial parallelisation.
- $\sim$300,000 nodes per vector found.
- Can heuristically analyze the miss rate and subtrees sizes via volumes of truncated hyperspheres.

- Resembles the "extreme pruning" from [Gama et al, Eurocrypt'10].

Concluding remarks

- Our code (in Magma/C) ran in 4 days using 14 CPUs.
- The data can be checked in about 10 hours on 1 CPU.
- ≈90% time in finding vectors, 5% canonical orbit reps.

- There are at least 3 other "candidates" for $n = 80$, though the **Aut** groups are not as nice.
- No extremal candidate is known (to us) for $n = 72$.
- We can prove that L is not isometric to the Bachoc-Nebe lattices, using the Classification of Finite Simple Groups.

- For more details, read the paper. ☺