Configurations of Extremal Type II Lattices and Codes

Scott Duke Kominers

Department of Economics, Harvard University, and Harvard Business School

AMS-MAA-SIAM Session on Research in Mathematics by Undergraduates
Joint Mathematics Meetings
January 15, 2010
Key Concepts
Key Concepts

lattice
Key Concepts

lattice
Key Concepts

lattice
Key Concepts

lattice
Key Concepts

lattice

“integer vector space”
Key Concepts

- lattice

- “integer vector space”
  - free $\mathbb{Z}$-module with an inner product
  \[ \langle \cdot, \cdot \rangle : L \times L \rightarrow \mathbb{R} \]
Key Concepts

- lattice

- “integer vector space”
- free $\mathbb{Z}$-module with an inner product
  \[ \langle \cdot, \cdot \rangle : L \times L \to \mathbb{R} \]
- rank $\sim$ size of basis
Key Concepts

lattice
Key Concepts

- **lattice** ∼ “integer vector space”
  - free $\mathbb{Z}$-module with an inner product $\langle \cdot, \cdot \rangle$
  - rank ∼ size of basis
Key Concepts

unimodular lattice

- **unimodular** \(\sim\) self-dual
  - basis matrix has determinant 1
- **lattice** \(\sim\) “integer vector space”
  - free \(\mathbb{Z}\)-module with an inner product \(\langle \cdot, \cdot \rangle\)
  - rank \(\sim\) size of basis
Key Concepts

- **even unimodular lattice**

  - **even** $\sim$ all vectors have even norm
    - $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$
  - **unimodular** $\sim$ self-dual
    - basis matrix has determinant 1
  - **lattice** $\sim$ “integer vector space”
    - free $\mathbb{Z}$-module with an inner product $\langle \cdot, \cdot \rangle$
    - rank $\sim$ size of basis
Key Concepts

- **even unimodular lattice**
  - Type II

- **even** \(\sim\) all vectors have even norm
  - \(\langle x, x \rangle \in 2\mathbb{Z}\) for all \(x \in L\)

- **unimodular** \(\sim\) self-dual
  - basis matrix has determinant 1

- **lattice** \(\sim\) “integer vector space”
  - free \(\mathbb{Z}\)-module with an inner product \(\langle \cdot, \cdot \rangle\)
  - rank \(\sim\) size of basis
Key Concepts

**even unimodular lattice**

- **even** \( \sim \) all vectors have even norm
  - \( \langle \mathbf{x}, \mathbf{x} \rangle \in 2\mathbb{Z} \) for all \( \mathbf{x} \in L \)
- **unimodular** \( \sim \) self-dual
  - basis matrix has determinant 1
- **lattice** \( \sim \) “integer vector space”
  - free \( \mathbb{Z} \)-module with an inner product \( \langle \cdot, \cdot \rangle \)
  - rank \( \sim \) size of basis
Key Concepts

extremal even unimodular lattice

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
  - $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$
- unimodular $\sim$ self-dual
  - basis matrix has determinant 1
- lattice $\sim$ “integer vector space”
  - free $\mathbb{Z}$-module with an inner product $\langle \cdot, \cdot \rangle$
  - rank $\sim$ size of basis
Key Concepts

extremal \textit{even unimodular} lattice Type II

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
  - $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$
- unimodular $\sim$ self-dual
  - basis matrix has determinant 1
- lattice $\sim$ “integer vector space”
  - free $\mathbb{Z}$-module with an inner product $\langle \cdot, \cdot \rangle$
  - rank $\sim$ size of basis
Key Concepts

extremal even unimodular lattice

Type II

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
  - $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$
- unimodular $\sim$ self-dual
  - basis matrix has determinant 1
- lattice $\sim$ “integer vector space”
  - free $\mathbb{Z}$-module with an inner product $\langle \cdot, \cdot \rangle$
  - rank $\sim$ size of basis
Key Concepts

extremal even unimodular lattice

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
- unimodular $\sim$ self-dual
- lattice $\sim$ “integer vector space”
  - rank $\sim$ size of basis
Key Concepts

extremal \underbrace{\text{even unimodular}} \text{ lattice} \quad \text{Type II}

- extremal \sim \text{shortest vector is as long as possible}
- even \sim \text{all vectors have even norm}
- unimodular \sim \text{self-dual}
- lattice \sim \text{“integer vector space”}
  - rank \sim \text{size of basis}
Key Concepts

extremal even unimodular lattice

Type II

- extremal \(\sim\) shortest vector is as long as possible
- even \(\sim\) all vectors have even norm
- unimodular \(\sim\) self-dual
- lattice \(\sim\) “integer vector space”
  - rank \(\sim\) size of basis

For a Type II lattice \(L\), \(\text{rank}(L) = 8n\)....
Key Concepts

extremal even unimodular lattice

Type II

- extremal \(\sim\) shortest vector is as long as possible
- even \(\sim\) all vectors have even norm
- unimodular \(\sim\) self-dual
- lattice \(\sim\) “integer vector space”
  - rank \(\sim\) size of basis

For a Type II lattice \(L\), \(\text{rank}(L) = 8n\).
Key Concepts

extremal even unimodular lattice

Type II

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
- unimodular $\sim$ self-dual
- lattice $\sim$ “integer vector space”
  - rank $\sim$ size of basis
Key Concepts

extremal $\underbrace{\text{even unimodular}}$ lattice

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
- unimodular $\sim$ self-dual
- lattice $\sim$ “integer vector space”
  - rank $\sim$ size of basis

Applications to sphere-packing problems
Key Concepts

extremal even unimodular lattice

- extremal \( \sim \) shortest vector is as long as possible
- even \( \sim \) all vectors have even norm
- unimodular \( \sim \) self-dual
- lattice \( \sim \) “integer vector space”
  - rank \( \sim \) size of basis

- Applications to \( \text{dim-}8n \) sphere-packing problems
Key Concepts

extremal even unimodular lattice

- extremal $\sim$ shortest vector is as long as possible
- even $\sim$ all vectors have even norm
- unimodular $\sim$ self-dual
- lattice $\sim$ “integer vector space”
  - rank $\sim$ size of basis

Applications to dim-$8n$ sphere-packing problems
Lattice Configuration Results
Lattice Configuration Results

Theorem
Lattice Configuration Results

Theorem Template
Lattice Configuration Results

Theorem Template

*If L is Type II and extremal of rank n, then the minimal-norm vectors of L generate L.*
Theorem Template

*If $L$ is Type II and extremal of rank $n$, then the minimal-norm vectors of $L$ generate $L$."

- Folklore: $n \in \{8, 24\}$
Lattice Configuration Results

Theorem Template

*If $L$ is Type II and extremal of rank $n$, then the minimal-norm vectors of $L$ generate $L$.***

- Folklore: $n \in \{8, 24\}$
- Venkov (1984): $n \in \{32\}$
Theorem Template

*If* $L$ *is Type II and extremal of rank* $n$, *then the minimal-norm vectors of* $L$ *generate* $L$.

- **Folklore:** $n \in \{8, 24\}$
- **Venkov (1984):** $n \in \{32\}$
- **Ozeki (1986):** $n \in \{32, 48\}$
Theorem Template

If $L$ is Type II and extremal of rank $n$, then the minimal-norm vectors of $L$ generate $L$.

- Folklore: $n \in \{8, 24\}$
- Venkov (1984): $n \in \{32\}$
- Ozeki (1986): $n \in \{32, 48\}$
- K. (2009): $n \in \{56, 72, 96\}$
Lattice Configuration Results

Theorem Template

If $L$ is Type II and extremal of rank $n$, then the minimal-norm vectors of $L$ generate $L$.

- Folklore: $n \in \{8, 24\}$
- Venkov (1984): $n \in \{32\}$
- Ozeki (1986): $n \in \{32, 48\}$
- K. (2009): $n \in \{56, 72, 96\}$
- Elkies (2010): $n \in \{120\}$
Theta Functions
Theta Functions

- **Slogan:**
  
  "The *theta function* of a lattice $L$ *encodes* the lengths of $L$’s vectors."
Theta Functions

- **Slogan:**
  
  "The theta function of a lattice $L$ encodes the lengths of $L$’s vectors."

- **How:**
  
  "norm $\langle x, x \rangle$" $\iff$ "length"
Theta Functions

- **Slogan:**
  
  "The theta function of a lattice $L$ encodes the lengths of $L$’s vectors."

- **How:**
  
  "norm $\langle x, x \rangle$” $\iff$ “length”

- **What:**

  \[
  \Theta_L(\tau) = \sum_{x \in L} e^{i\pi\tau \langle x, x \rangle} = \sum_{k=1}^{\infty} a_k e^{i\pi\tau(k)}
  \]
Theta Functions

Slogan: “The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors.”
Theta Functions

- Slogan:
  "The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors."

- Example:
Theta Functions

- **Slogan:**
  
  “The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors.”

- **Example:**

  ![Diagram of a lattice with theta function example](image)
Theta Functions

- **Slogan:**
  "The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors."

- **Example:**

$$\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi \tau \langle x, x \rangle}$$
Theta Functions

- **Slogan:**
  "The theta function \( \sum_{x \in L} e^{i\pi \tau \langle x, x \rangle} \) of a lattice \( L \) encodes the lengths of \( L \)'s vectors."

- **Example:**

\[
\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi \tau \langle x, x \rangle} = 1 + 4e^{i\pi \tau} + 4e^{2i\pi \tau}
\]
Theta Functions

- **Slogan:**
  “The theta function \( \sum_{x \in L} e^{i\pi \tau \langle x, x \rangle} \) of a lattice \( L \) encodes the lengths of \( L \)'s vectors.”

- **Example:**

\[
\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi \tau \langle x, x \rangle} = 1 + 4e^{i\pi \tau} + 4e^{2i\pi \tau} + 0e^{3i\pi \tau} + 4e^{4i\pi \tau}
\]
Theta Functions

- **Slogan:**
  “The theta function \( \sum_{x \in L} e^{i\pi \tau \langle x, x \rangle} \) of a lattice \( L \) encodes the lengths of \( L \)’s vectors.”

- **Example:**

\[
\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi \tau \langle x, x \rangle}
= 1 + 4e^{i\pi \tau} + 4e^{2i\pi \tau} \\
+ 0e^{3i\pi \tau} + 4e^{4i\pi \tau} \\
+ 8e^{4i\pi \tau} + \cdots
\]
Theta Functions

- Slogan:
  “The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors.”
Theta Functions

- **Slogan:**
  
  “The theta function \( \sum_{x \in L} e^{i \pi \tau \langle x, x \rangle} \) of a lattice \( L \) encodes the lengths of \( L \)’s vectors.”

- **Why we care:**
  
  - For \( L \) Type II of rank \( n \), the theta function \( \Theta_L \) is a modular form: \( \Theta_L \in \mathcal{M}_{n/2} \).
Theta Functions

- **Slogan:**
  
  “The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors.”

- **Why we care:**
  
  - For $L$ Type II of rank $n$, the theta function $\Theta_L$ is a modular form: $\Theta_L \in \mathcal{M}_{n/2}$.
  - For $n$ small, the space $\mathcal{M}_{n/2}$ is small.
Theta Functions

- **Slogan:**
  “The theta function $\sum_{x \in L} e^{i\pi \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors.”

- **Why we care:**
  - For $L$ Type II of rank $n$, the theta function $\Theta_L$ is a modular form: $\Theta_L \in M_{n/2}$.
  - For $n$ (relatively) small, the space $M_{n/2}$ is (very) small.
Theta Functions

- **Slogan:**
  
  “The theta function \( \sum_{x \in L} e^{i\pi \tau \langle x, x \rangle} \) of a lattice \( L \) encodes the lengths of \( L \)'s vectors.”

- **Why we care:**
  
  - For \( L \) Type II of rank \( n \), the theta function \( \Theta_L \) is a modular form: \( \Theta_L \in \mathcal{M}_{n/2} \).
  
  - For \( n \) (relatively) small, the space \( \mathcal{M}_{n/2} \) is (very) small.
Theta Functions

- Slogan:
  "The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ encodes the lengths of $L$’s vectors."

- Why we care:
  - For $L$ Type II of rank $n$, the theta function $\Theta_L$ is a modular form: $\Theta_L \in \mathcal{M}_{n/2}$.
  - For $n$ (relatively) small, the space $\mathcal{M}_{n/2}$ is (very) small.
  - We can therefore study the function $\Theta_L$ even if we cannot write down a basis for $L$. 
Slogan:

“The theta function \( \sum_{x \in L} e^{i\pi \tau \langle x, x \rangle} \) of a lattice \( L \) is a modular form which encodes the lengths of \( L \)’s vectors.”
Theta Functions

- Slogan:
  "The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ is a modular form which encodes the lengths of $L$'s vectors."

- What we do:
Theta Functions

- **Slogan:**
  "The theta function $\sum_{x \in L} e^{i\pi \tau \langle x, x \rangle}$ of a lattice $L$ is a modular form which encodes the lengths of $L$’s vectors."

- **What we do:**
  - We study weighted theta functions $\sum_{x \in L} P(x) e^{i\pi \tau \langle x, x \rangle}$ which encode norms and distributions of lattice vectors.
Theta Functions

- **Slogan:**
  
  “The *theta function* \( \sum_{x \in L} e^{i\pi \tau \langle x, x \rangle} \) of a lattice \( L \) is a *modular form* which *encodes* the lengths of \( L \)’s vectors.”

- **What we do:**
  
  - We study *weighted theta functions* \( \sum_{x \in L} P(x) e^{i\pi \tau \langle x, x \rangle} \) which encode norms and distributions of lattice vectors.
  
  - We obtain a “system of equations in vector distributions” which proves our configuration results.
Lattice Configuration Results

Theorem Template

*If L is Type II and extremal of rank n, then the minimal-norm vectors of L generate L.*

- **Folklore:** $n \in \{8, 24\}$
- **Venkov (1984):** $n \in \{32\}$
- **Ozeki (1986):** $n \in \{32, 48\}$
- **K. (2009):** $n \in \{56, 72, 96\}$
- **Elkies (2010):** $n \in \{120\}$
Theorem Template

If $L$ is Type II and extremal of rank $n$, then the minimal-norm vectors of $L$ generate $L$.

- Folklore: $n \in \{8, 24\}$
- Venkov (1984): $n \in \{32\}$
- Ozeki (1986): $n \in \{32, 48\}$
- K. (2009): $n \in \{56, 72, 96\}$
- Elkies (2010): $n \in \{120\}$
Lattice Configuration Results

Theorem Template

If $L$ is Type II and extremal of rank $n$ with minimal norm $m_L$, then $L$ is generated by its vectors of norms $m_L$ and $(m_L + 2)$.

Folklore:

$n \in \{16\}$

Ozeki (1989):

$n \in \{40\}$


$n \in \{40, 80, 120\}$ (unified method)

Elkies–K. (2010): Norm-$(m_L + 2)$ suffices for $n \in \{40, 80\}$
Lattice Configuration Results

Theorem Template

If $L$ is Type II and extremal of rank $n$ with minimal norm $m(L)$, then $L$ is generated by its vectors of norms $m(L)$ and $(m(L) + 2)$. 
Theorem Template

If $L$ is Type II and extremal of rank $n$ with minimal norm $m(L)$, then $L$ is generated by its vectors of norms $m(L)$ and $(m(L) + 2)$.

- Folklore: $n \in \{16\}$
Theorem Template

If $L$ is Type II and extremal of rank $n$ with minimal norm $m(L)$, then $L$ is generated by its vectors of norms $m(L)$ and $(m(L) + 2)$.

- Folklore: $n \in \{16\}$
- Ozeki (1989): $n \in \{40\}$
Theorem Template

*If* $L$ *is Type II and extremal of rank* $n$ *with minimal norm* $m(L)$, *then* $L$ *is generated by its vectors of norms* $m(L)$ *and* $(m(L) + 2)$.

- Folklore: $n \in \{16\}$
- Ozeki (1989): $n \in \{40\}$
- Abel–K. (2008): $n \in \{40, 80, 120\}$ (unified method)
Lattice Configuration Results

Theorem Template

If $L$ is Type II and extremal of rank $n$ with minimal norm $m(L)$, then $L$ is generated by its vectors of norms $m(L)$ and $(m(L) + 2)$.

- Folklore: $n \in \{16\}$
- Ozeki (1989): $n \in \{40\}$
- Abel–K. (2008): $n \in \{40, 80, 120\}$ (unified method)
- Elkies–K. (2010): Norm-$(m(L) + 2)$ suffices for $n \in \{40, 80\}$
Pause
We just described configurations of lattices.
We just described configurations of lattices.
Recall the title slide....
Configurations of Extremal Type II Lattices and Codes

Scott Duke Kominers

Department of Economics, Harvard University, and Harvard Business School

AMS-MAA-SIAM Session on Research in Mathematics by Undergraduates
Joint Mathematics Meetings
January 15, 2010
We just described configurations of lattices.
Recall the title slide....
We just described configurations of lattices.

Recall the title slide....

Natural Question
We just described configurations of lattices.

Recall the title slide....

Natural Question

What about codes?
Key Concepts

extremal even unimodular lattice

Type II
Key Concepts

extremal \textit{even unimodular} lattice

Type II

extremal \textit{doubly-even self-dual} code

Type II
Key Concepts

extremal even unimodular lattice

Type II

- lattice of rank $n \sim$ “integer vector space” of rank $n$
- code of length $n \sim$ linear subspace of $\mathbb{F}_2^n$

extremal doubly-even self-dual code

Type II
Key Concepts

- extremal even unimodular lattice
- unimodular $\sim$ self-dual
- self-dual $\sim$ self-dual

- extremal doubly-even self-dual code

Type II
Key Concepts

extremal even unimodular lattice

- even \( \sim \) all vectors have even norm
- doubly-even \( \sim \) 4 divides all codewords’ weights

extremal doubly-even self-dual code
Key Concepts

extremal even unimodular lattice

Type II

extremal doubly-even self-dual code

Type II
Key Concepts

extremal even unimodular lattice

- extremal $\sim$ shortest vector is as long as possible
- extremal $\sim$ smallest codeword is as large as possible

extremal doubly-even self-dual code

Type II
Key Concepts

- Extremal even unimodular lattice
- Type II

- Extremal doubly-even self-dual code
- Type II
Key Concepts

extremal even unimodular lattice

Type II

Construction A

extremal doubly-even self-dual code

Type II
Weight Enumerators

- Theta Function Slogan:

  “The \textit{theta function} $\Theta_L(\tau)$ of a lattice $L$ \textit{encodes} the lengths of $L$’s vectors.”
Weight Enumerators

• Theta Function Slogan: “The \( \theta \) function \( \Theta_L(\tau) \) of a lattice \( L \) encodes the lengths of \( L \)'s vectors.”

• Weight Enumerator Slogan: “The weight enumerator \( W_C(x, y) \) of a code \( C \) encodes the weights of \( C \)'s codewords.”
Weight Enumerators

- **Theta Function Slogan:**
  “The *theta function* $\Theta_L(\tau)$ of a lattice $L$ is a *modular form* which *encodes* the lengths of $L$’s vectors.”

- **Weight Enumerator Slogan:**
  “The *weight enumerator* $W_C(x, y)$ of a code $C$ *encodes* the weights of $C$’s codewords.”
Weight Enumerators

- **Theta Function Slogan:**
  
  "The *theta function* $\Theta_L(\tau)$ of a lattice $L$ is a *modular form* which *encodes* the lengths of $L$’s vectors."

- **Weight Enumerator Slogan:**
  
  "The *weight enumerator* $W_C(x, y)$ of a code $C$ *encodes* the weights of $C$’s codewords."
Weight Enumerators

- **Theta Function Slogan:**
  “The *theta function* $\Theta_L(\tau)$ of a lattice $L$ is a *modular form* which *encodes* the lengths of $L$’s vectors.”

- **Weight Enumerator Slogan:**
  “The *weight enumerator* $W_C(x, y)$ of a code $C$ is a *classifiable* polynomial which *encodes* the weights of $C$’s codewords.”
Weight Enumerators

Theta Function Slogan:
“The theta function $\Theta_L(\tau)$ of a lattice $L$ is a modular form which encodes the lengths of $L$’s vectors.”

Weight Enumerator Slogan:
“The weight enumerator $W_C(x, y)$ of a code $C$ is a classifiable polynomial which encodes the weights of $C$’s codewords.”
Weight Enumerators

- **Theta Function Slogan:**
  
  "The *weighted theta function* $\Theta_{L,P}(\tau)$ of $L$ is a *modular form* which *encodes* the distributions of $L$’s vectors."

- **Weight Enumerator Slogan:**
  
  "The *harmonic weight enumerator* $W_{C,Q}(x,y)$ of $C$ is a classifiable polynomial which *encodes* the distributions of $C$’s codewords."
Weight Enumerators

- **Theta Function Slogan:**
  "The weighted theta function $\Theta_{L,P}(\tau)$ of $L$ is a modular form which encodes the distributions of $L$’s vectors."

- **Weight Enumerator Slogan:**
  "The harmonic weight enumerator $W_{C,Q}(x,y)$ of $C$ is a classifiable polynomial which encodes the distributions of $C$’s codewords."
Theorem Template

If $C$ is Type II and extremal of length $n$, then the minimal-weight codewords of $C$ generate $C$.

Folklore(?):

$n \in \{8, 24\}$

K. (2009):

$n \in \{32, 48, 56, 72, 96\}$

Likely: Analog of slightly weaker result for $n \in \{40, 80, 120\}$
Theorem Template

If $C$ is Type II and extremal of length $n$, then the minimal-weight codewords of $C$ generate $C$. 
Theorem Template

If $C$ is Type II and extremal of length $n$, then the minimal-weight codewords of $C$ generate $C$.

- Folklore(?): $n \in \{8, 24\}$
Theorem Template

*If C is Type II and extremal of length n, then the minimal-weight codewords of C generate C.*

- Folklore(?): \( n \in \{8, 24\} \)
- K. (2009): \( n \in \{32, 48, 56, 72, 96\} \)
Theorem Template

If $C$ is Type II and extremal of length $n$, then the minimal-weight codewords of $C$ generate $C$.

- Folklore(?): $n \in \{8, 24\}$
- K. (2009): $n \in \{32, 48, 56, 72, 96\}$
- Likely: Analog of slightly weaker result for $n \in \{40, 80, 120\}$
Conclusion
Conclusion

Lattices

Codes
Conclusion

Lattices

common

Codes
Conclusion

Lattices

common

uncommon

Codes
Acknowledgments
Acknowledgments

- Prof. Noam D. Elkies
Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
- Harvard College \{PRISE, Highbridge\} Fellowships
Acknowledgments

Prof. Noam D. Elkies
Mrs. Susan Schwartz Wildstrom
Harvard College \{PRISE, Highbridge\} Fellowships

AMS, MAA, and SIAM
Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
- Harvard College {PRISE, Highbridge} Fellowships
- AMS, MAA, and SIAM
- Advisors
Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
- Harvard College \{PRISE, Highbridge\} Fellowships
- AMS, MAA, and SIAM
- Advisors, family
Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
- Harvard College \{PRISE, Highbridge\} Fellowships
- AMS, MAA, and SIAM
- Advisors, family, friends
 Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
- Harvard College \{PRISE, Highbridge\} Fellowships
- AMS, MAA, and SIAM
- Advisors, family, friends, and you!
Acknowledgments

- Prof. Noam D. Elkies
- Mrs. Susan Schwartz Wildstrom
- Harvard College \{PRISE, Highbridge\} Fellowships
- AMS, MAA, and SIAM
- Advisors, family, friends, and you! (QED)
Questions?

http://www.scottkom.com/
Extra Slides
**Example Code**

The codewords of the *extended Hamming code* $e_8$ are given by the columns of the matrix

\[
\begin{pmatrix}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}.
\]
Theta Function Conditions: $n = 72$ Case

Fix an equivalence class $[x_0]$ where $\langle x_0, x_0 \rangle = 2t$ ($t \geq 5$) is minimal for some $t \geq 5$.

For all $x \in \Lambda_8(L)$, we have $|\langle x_0, x \rangle| \leq 4$.

$\Theta L, P \equiv 0$ for $0 < (\deg P) / 2 \leq 5$.

$\sum_{x \in \Lambda_8(L)} \langle x, x_0 \rangle^2 = 2 \sum_{j=1}^{4} N_j(x_0)$. 

$6218175600 = |\Lambda_8(L)| = N_0(x_0) + 2 \sum_{j=1}^{4} N_j(x_0)$.

$2 \cdot 25^3 = 168^2 t^4 - 2800 t^3 + 17745 t^2 - 50635 t + 54834 = 0 \Rightarrow t = 0 \Rightarrow \cdots$. 

Scott Duke Kominers (Harvard)
January 15, 2010
Theta Function Conditions: $n = 72$ Case

- Fix an equivalence class $[x_0]$ where $\langle x_0, x_0 \rangle = 2t$ ($t \geq 5$) is minimal for some $t \geq 5$. 

\[ 6218175600 = |\Lambda_{8}(L)| = N_{0}(x_0) + 2 \sum_{4 \leq j \leq 5} N_{j}(x_0). \]

\[ 2t(168t^4 - 2800t^3 + 17745t^2 - 50635t + 54834) = 0 \Rightarrow t = 0 \Rightarrow \text{false}. \]
Theta Function Conditions: \( n = 72 \) Case

- Fix an equivalence class \([x_0]\) where \( \langle x_0, x_0 \rangle = 2t \) (\( t \geq 5 \)) is minimal for some \( t \geq 5 \).
- For all \( x \in \Lambda_8(L) \), we have \( |\langle x_0, x \rangle| \leq 4 \).
Theta Function Conditions: $n = 72$ Case

- Fix an equivalence class $[x_0]$ where $\langle x_0, x_0 \rangle = 2t$ ($t \geq 5$) is minimal for some $t \geq 5$.
- For all $x \in \Lambda_8(L)$, we have $|\langle x_0, x \rangle| \leq 4$.
- $\Theta_{L,P} \equiv 0$ for $0 < (\deg P)/2 \leq 5$.
- $\sum_{x \in \Lambda_8(L)} \langle x, x_0 \rangle^{2k} = 2 \sum_{j=1}^{4} j^{2k} \cdot N_j(x_0)$. 
Theta Function Conditions: \( n = 72 \) Case

- Fix an equivalence class \([x_0]\) where \( \langle x_0, x_0 \rangle = 2t \) \((t \geq 5)\) is minimal for some \( t \geq 5 \).
- For all \( x \in \Lambda_8(L) \), we have \(|\langle x_0, x \rangle| \leq 4\).
- \( \Theta_{L,P} \equiv 0 \) for \( 0 < (\deg P)/2 \leq 5 \).
- \( \sum_{x \in \Lambda_8(L)} \langle x, x_0 \rangle^{2k} = 2 \sum_{j=1}^{4} j^{2k} \cdot N_j(x_0) \).
- \( 6218175600 = |\Lambda_8(L)| = N_0(x_0) + 2 \sum_{j=1}^{4} N_j(x_0) \).
Theta Function Conditions: $n = 72$ Case

- Fix an equivalence class $[x_0]$ where $\langle x_0, x_0 \rangle = 2t$ ($t \geq 5$) is minimal for some $t \geq 5$.
- For all $x \in \Lambda_8(L)$, we have $|\langle x_0, x \rangle| \leq 4$.
- $\Theta_{L,P} \equiv 0$ for $0 < (\text{deg } P)/2 \leq 5$.
- $\sum_{x \in \Lambda_8(L)} \langle x, x_0 \rangle^{2k} = 2 \sum_{j=1}^{4} j^{2k} \cdot N_j(x_0)$.
- $6218175600 = |\Lambda_8(L)| = N_0(x_0) + 2 \sum_{j=1}^{4} N_j(x_0)$.
- $2^{25}3^95^47^2t(168t^4 - 2800t^3 + 17745t^2 - 50635t + 54834) = 0 \Rightarrow t = 0 \Rightarrow \Leftarrow$. 