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

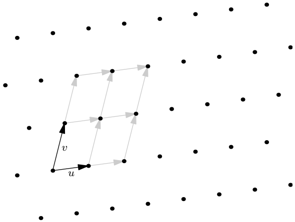
Key Concepts

Key Concepts

lattice

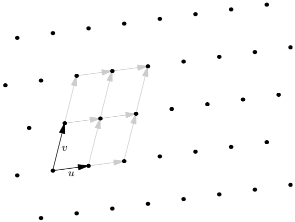
Key Concepts

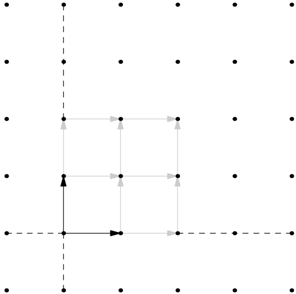
lattice



Key Concepts

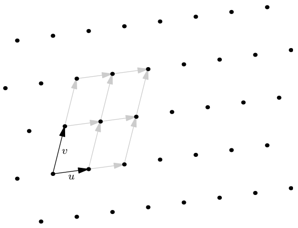
lattice





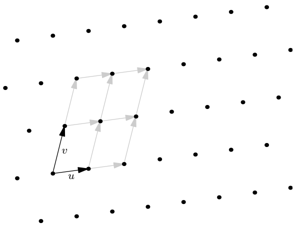
Key Concepts

lattice



Key Concepts

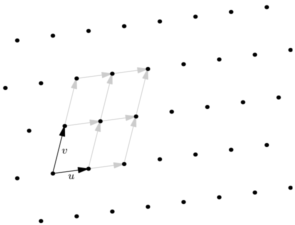
lattice



- "integer vector space"

Key Concepts

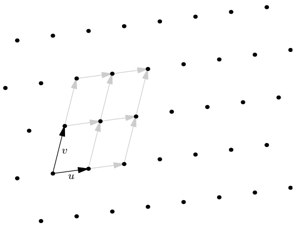
lattice



- "integer vector space"
  - free $\mathbb{Z}$-module with an inner product $\langle \cdot, \cdot \rangle : L \times L \to \mathbb{R}$

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

- 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

$$\underbrace{\text{even unimodular}}_{\text{Type II}}\ \text{lattice}$$

- 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

$$\underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- 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

$$\text{extremal}\ \underbrace{\text{even unimodular}}_{\text{Type II}}\ \text{lattice}$$

- 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

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

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

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- 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

$$\text{extremal}\ \underbrace{\text{even unimodular}}_{\text{Type II}}\ \text{lattice}$$

- extremal ~ shortest vector is as long as possible
- even ~ all vectors have even norm
- unimodular ~ self-dual
- lattice ~ "integer vector space"
  - rank ~ size of basis

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

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

Key Concepts

$$\text{extremal}\ \underbrace{\text{even unimodular}}_{\text{Type II}}\ \text{lattice}$$

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

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

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

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

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

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- 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

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- extremal ∼ shortest vector is as long as possible
- even ∼ all vectors have even norm
- unimodular ∼ self-dual
- lattice ∼ "integer vector space"
  - rank ∼ size of basis
- Applications to dim-8n sphere-packing problems

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- extremal ∼ shortest vector is as long as possible
- even ∼ all vectors have even norm
- unimodular ∼ self-dual
- lattice ∼ "integer vector space"
  - rank ∼ 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.

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

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): $n \in \{32\}$

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): $n \in \{32, 48\}$

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): $n \in \{56, 72, 96\}$

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:

  $$\text{“norm } \langle x, x\rangle\text{”} \iff \text{“length”}$$

Theta Functions

- Slogan:

  "The *theta function* of a lattice L *encodes* the lengths of L's vectors."

- How:

  $$\text{“norm } \langle x, x \rangle\text{”} \iff \text{“length”}$$

- 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:

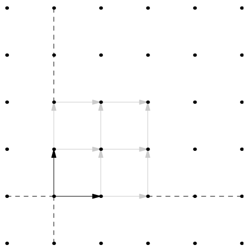
  "The *theta function* $\sum_{x \in L} e^{i\pi\tau\langle x,x\rangle}$ of a lattice L *encodes* the lengths of L's vectors."

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:

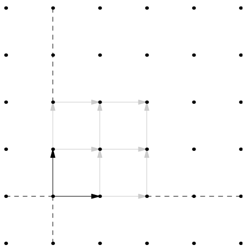


Theta Functions

- 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:



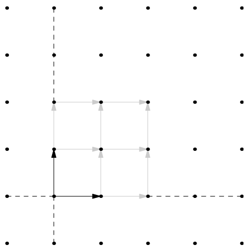
$$\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi\tau\langle x,x\rangle}$$

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:



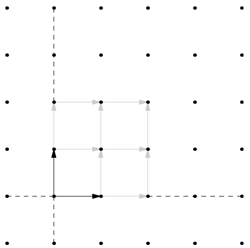
$$\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi\tau\langle x,x\rangle}$$
$$= 1 + 4e^{i\pi\tau} + 4e^{2i\pi\tau}$$

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:



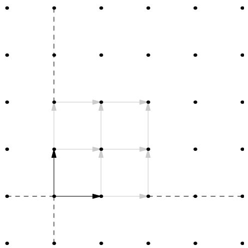
$$\Theta_{\mathbb{Z}^2}(\tau) = \sum_{x \in \mathbb{Z}^2} e^{i\pi\tau\langle x,x\rangle}$$
$$= 1 + 4e^{i\pi\tau} + 4e^{2i\pi\tau} + 0e^{3i\pi\tau} + 4e^{4i\pi\tau}$$

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:



$$\begin{aligned}\Theta_{\mathbb{Z}^2}(\tau) = & \sum_{x \in \mathbb{Z}^2} e^{i\pi\tau\langle x,x\rangle} \\ = & 1 + 4e^{i\pi\tau} + 4e^{2i\pi\tau} \\ & + 0e^{3i\pi\tau} + 4e^{4i\pi\tau} \\ & + 8e^{4i\pi\tau} + \cdots\end{aligned}$$

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 Θ_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 Θ_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* $\sum_{x \in L} e^{i\pi\tau\langle x,x\rangle}$ of a lattice L *encodes* the lengths of L's vectors."

- Why we care:
  - For L Type II of rank n, the theta function Θ_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 Θ_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 Θ_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 Θ_L even if we cannot write down a basis for L.

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."

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): $n \in \{120\}$

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): $n \in \{120\}$

Lattice Configuration Results

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 $(m(L) + 2)$.

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: $n \in \{16\}$

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): $n \in \{40\}$

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)

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

Pause

- We just described configurations of lattices.

Pause

- We just described configurations of lattices.
- Recall the title slide....

Pause

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

Pause

- We just described configurations of lattices.
- Recall the title slide....

Pause

- We just described configurations of lattices.
- Recall the title slide....

Natural Question

Pause

- We just described configurations of lattices.
- Recall the title slide....

Natural Question

What about codes?

Key Concepts

extremal $\underbrace{\text{even unimodular}}_{\text{Type II}}$ lattice

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

$$\text{extremal } \underbrace{\text{doubly-even self-dual}}_{\text{Type II}} \text{ code}$$

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

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

$$\text{extremal } \underbrace{\text{doubly-even self-dual}}_{\text{Type II}} \text{ code}$$

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- unimodular ∼ self-dual
- self-dual ∼ self-dual

$$\text{extremal } \underbrace{\text{doubly-even self-dual}}_{\text{Type II}} \text{ code}$$

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

- even $\sim$ all vectors have even norm
- doubly-even $\sim$ 4 divides all codewords' weights

$$\text{extremal } \underbrace{\text{doubly-even self-dual}}_{\text{Type II}} \text{ code}$$

Key Concepts

extremal $\underbrace{\text{even unimodular}}_{\text{Type II}}$ lattice

extremal $\underbrace{\text{doubly-even self-dual}}_{\text{Type II}}$ code

Key Concepts

extremal $\underbrace{\text{even unimodular}}_{\text{Type II}}$ lattice

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

extremal $\underbrace{\text{doubly-even self-dual}}_{\text{Type II}}$ code

Key Concepts

$$\text{extremal } \underbrace{\text{even unimodular}}_{\text{Type II}} \text{ lattice}$$

$$\text{extremal } \underbrace{\text{doubly-even self-dual}}_{\text{Type II}} \text{ code}$$

Key Concepts

extremal even unimodular lattice

(even unimodular = Type II)

↑ Construction A

extremal doubly-even self-dual code

(doubly-even self-dual = Type II)

Weight Enumerators

- Theta Function Slogan:

  "The *theta function* $\Theta_L(\tau)$ of a lattice L *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."

Code Configuration Results

Code Configuration Results

Theorem Template

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

Code Configuration Results

Theorem Template

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

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

Code Configuration Results

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

Code Configuration Results

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

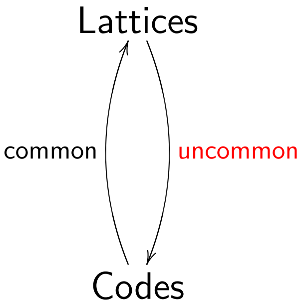
Conclusion

Lattices

common

Codes

Conclusion



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)

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

Theta Function Conditions: $n = 72$ Case

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

Theta Function Conditions: $n = 72$ Case

- Fix an equivalence class $[x_0]$ where $\langle x_0, x_0 \rangle = 2t$ $(t \geq 5)$ is mimimal 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 mimimal 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 mimimal 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 mimimal 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 $0 < (\deg P)/2 \leq 5$.
- $\sum_{x \in \Lambda_8(L)} \langle x, x_0 \rangle^{2k} = 2 \sum_{j=1}^{4} j^{2k} \cdot N_j(x_0)$.
- $6218175600 = |\Lambda_8(L)| = N_0(x_0) + 2 \sum_{j=1}^{4} N_j(x_0)$.
- $2^{25}3^9 5^4 7^2 t(168t^4 - 2800t^3 + 17745t^2 - 50635t + 54834) = 0 \Rightarrow t = 0 \Rightarrow\Leftarrow$.