# Designs and lattices: some applications.

Gabriele Nebe

Lehrstuhl D für Mathematik

EPF Lausanne, 21.7.2009

# The indecomposable root lattices.

## Theorem.

Let $L$ be an even lattice generated by its roots

$$R(L) = \{\ell \in L \mid Q(\ell) = \frac{1}{2}(\ell, \ell) = 1\}$$

then $L$ is orthogonal sum of the following indecomposable root lattices:

| $L$ | $\lvert R(L)\rvert$ | $h$ | $\det(L)$ | $L^{\#}/L$ | $n$ |
|---|---|---|---|---|---|
| $\mathbb{A}_n$ | $n(n+1)$ | $n+1$ | $n+1$ | $\mathbb{Z}/(n+1)\mathbb{Z}$ | $\geq 1$ |
| $\mathbb{D}_n$ | $2n(n-1)$ | $2(n-1)$ | 4 | $\mathbb{Z}/4\mathbb{Z}$ | $\geq 4$, odd |
| $\mathbb{D}_n$ | $2n(n-1)$ | $2(n-1)$ | 4 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ | $\geq 4$, even |
| $\mathbb{E}_6$ | 72 | 12 | 3 | $\mathbb{Z}/3\mathbb{Z}$ | 6 |
| $\mathbb{E}_7$ | 126 | 18 | 2 | $\mathbb{Z}/2\mathbb{Z}$ | 7 |
| $\mathbb{E}_8$ | 240 | 30 | 1 | 1 | 8 |

# Lattices and spherical designs.

## Remember.

- $$\begin{array}{lll} (D4) & \sum_{x\in X}(x,\alpha)^4 & = \frac{3|X|m^2}{n(n+2)}(\alpha,\alpha)^2 \\ (D2) & \sum_{x\in X}(x,\alpha)^2 & = \frac{|X|m}{n}(\alpha,\alpha) \end{array}$$

  for all $\alpha \in \mathbb{R}^n$ where $m = \min(L)$.
- A lattice $L$ is strongly perfect if $X = \mathrm{Min}(L)$ is a spherical 5-design, so if $X$ satisfies $(D4)$.
- A lattice $L$ is strongly eutactic if $X = \mathrm{Min}(L)$ is a spherical 3-design, so if $X$ satisfies $(D2)$.
- Indecomposable root lattices are strongly eutactic.
- A decomposable root lattice $L = R_1 \perp \ldots \perp R_s$ is strongly eutactic, iff $h(R_1) = \ldots = h(R_s)$.

# Even unimodular lattices of dimension 24.

## Remember.

Let $L = L^{\#} \in \mathcal{L}_n$ be an even unimodular lattice and $p \in \mathbb{R}[x_1, \ldots, x_n]$, $\deg(p) = t > 0$, $\Delta(p) = 0$. Then

$$\theta_{L,p} := \sum_{\ell \in L} p(\ell) q^{Q(\ell)} = \sum_{j=1}^{\infty} \left( \sum_{\ell \in L_j} p(\ell) \right) q^j \in M^0_{n/2+t}.$$

If $2m = \min(L)$ then $\theta_{L,p}$ is divisible by $\Delta^m \in M^0_{12m}$.

## Application for $n = 24$.

Know that $M^0_{14} = \{0\}$ so if $L$ is an even 24-dimensional unimodular lattice and $p$ a harmonic polynomial of degree 2, then $\theta_{L,p} = 0$.
In particular all even unimodular 24-dimensional lattices are strongly eutactic.

# Venkov's classication of the even unimodular lattices of dimension 24.

## Theorem (Venkov).

Let $L$ be an even unimodular lattice of dimension 24.

- The root system $R(L)$ is either empty or has full rank.
- The indecomposable components of $R(L)$ have the same Coxeter number.

Proof. Assume that $R(L) \neq \emptyset$. Since $L$ is strongly eutactic

$$\sum_{x \in R(L)} (x, \alpha)^2 = \frac{|R(L)|}{12}(\alpha, \alpha) \text{ for all } \alpha \in \mathbb{R}^{24}$$

In particular $R(L)^{\perp} = \{0\}$.
If $R(L) = R_1 \perp \ldots \perp R_s$, $n_i = \dim(R_i)$, and $\alpha \in \langle R_i \rangle_{\mathbb{R}}$, then

$$\sum_{x \in R(L)} (x, \alpha)^2 = \sum_{x \in R_i} (x, \alpha)^2 = \frac{2|R_i|}{n_i}(\alpha, \alpha).$$

Hence $h(R_i) = \frac{|R_i|}{n_i} = \frac{|R(L)|}{24}$ is independent of $i$.

# The even unimodular lattices of dimension 24.

The possible root systems are found combinatorically from the classification of indecomposable root systems and their Coxeter numbers:

$$\emptyset,\ 24\mathbb{A}_1,\ 12\mathbb{A}_2,\ 8\mathbb{A}_3,\ 6\mathbb{A}_4,\ 4\mathbb{A}_6,\ 3\mathbb{A}_8,\ 2\mathbb{A}_{12},\ \mathbb{A}_{24},$$
$$6\mathbb{D}_4,\ 4\mathbb{D}_6,\ 3\mathbb{D}_8,\ 2\mathbb{D}_{12},\ \mathbb{D}_{24},\ 4\mathbb{E}_6,\ 3\mathbb{E}_8,$$
$$4\mathbb{A}_5 \perp \mathbb{D}_4,\ 2\mathbb{A}_7 \perp 2\mathbb{D}_5,\ 2\mathbb{A}_9 \perp \mathbb{D}_6,\ \mathbb{A}_{15} \perp \mathbb{D}_9,$$
$$\mathbb{E}_8 \perp \mathbb{D}_{16}, 2\mathbb{E}_7 \perp \mathbb{D}_{10},\ \mathbb{E}_7 \perp \mathbb{A}_{17},\ \mathbb{E}_6 \perp \mathbb{D}_7 \perp \mathbb{A}_{11}$$

## Theorem.

For each of the 24 possible root systems there is a unique even unimodular lattice in dimension 24 having this root system.

# Proof of Theorem for $R \neq \emptyset$.

Proof. Let $M := \langle R(L) \rangle_{\mathbb{Z}} \subset L = L^{\#} \subset M^{\#}$. The inner product induces a bilinear form

$$b_M : M^{\#}/M \times M^{\#}/M \to \mathbb{Q}/\mathbb{Z}, (x + M, y + M) \mapsto (x, y) + \mathbb{Z}$$

with associated quadratic form

$$q_M : M^{\#}/M \to \mathbb{Q}/\mathbb{Z}, x + M \mapsto Q(x) + \mathbb{Z} = \frac{1}{2}(x, x) + \mathbb{Z}.$$

The even unimodular lattices $L$ that contain $M$ correspond to totally isotropic self-dual subgroups

$$(L/M)^{\perp} = L/M \leq M^{\#}/M \text{ with } q_M(L/M) = \{0\}.$$

$R(L) = R(M)$ iff for all $\ell \in L - M$,

$$\min(\ell + M) = \min\{2Q(\ell + m) \mid m \in M\} \geq 4.$$

# Example. Root system $6\mathbb{A}_4$.

$\mathbb{A}_4^{\#}/\mathbb{A}_4 = \langle x \rangle \cong \mathbb{F}_5$.

$\mathbb{A}_4^{\#} = \langle \mathbb{A}_4, x \rangle$ with $\min(ax + \mathbb{A}_4) = \begin{cases} 4/5 & \text{for } a = 1, -1 \\ 6/5 & \text{for } a = 2, -2 \end{cases}$.

Unimodular overlattices of $6\mathbb{A}_4$ correspond to self-dual codes $C = C^{\perp} \leq \mathbb{F}_5^6$.

$$C_1 : \begin{bmatrix} 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 \end{bmatrix}, \; C_2 : \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 & 2 & 1 \end{bmatrix}$$

yield the lattices

$$L_1 = \langle 6\mathbb{A}_4, x_1 + 2x_4, x_2 + 2x_5, x_3 + 2x_6 \rangle \cong 4\mathbb{E}_8$$

$$L_2 = \langle 6\mathbb{A}_4, x_1 + 2x_4 + x_5 + 2x_6, x_2 + x_4 + 2x_5 + 3x_6, x_3 + 3x_4 + 2x_5 + x_6 \rangle$$

with $R(L_2) = 6\mathbb{A}_4$.

# 24-dimensional even unimodular lattices.

## Theorem.

For each of the 24 possible root systems there is a unique even unimodular lattice in dimension 24 having this root system.

## Remark.

The uniqueness of the Leech lattice, the unique even unimodular lattice of dimension 24 with no roots is proven differently. It follows for instance from the uniqueness of the Golay code, but also by applying the mass formula:

$$\sum_{i=1}^{h} |\operatorname{Aut}(L_i)|^{-1} = m_{2k} = \frac{|B_k|}{2k} \prod_{j=1}^{k-1} \frac{B_{2j}}{4j}$$

where $L_1, \ldots, L_h$ represent the isometry classes of even unimodular lattices in $\mathbb{R}^{2k}$.

$$m_{24} = \frac{1027637932586061520960267}{129477933340026851560636148613120000000}$$

# Some applications of representation theory.

- Recall that the automorphism group of a lattice $L$ is $G := \mathrm{Aut}(L) = \{\sigma \in O_n(\mathbb{R}) \mid \sigma(L) = L\}$.
- $G$ acts on $L_a = \{\ell \in L \mid \frac{1}{2}(\ell, \ell) = Q(\ell) = a\}$.
- In particular $\mathrm{Min}(L)$ is a union of $G$ orbits.
- $$\alpha \mapsto \sum_{x \in \mathrm{Min}(L)} (x, \alpha)^d$$
  is a $G$-invariant polynomial of degree $d$.
- $\mathrm{Inv}_d(G) := \{p \in \mathbb{R}[x_1, \ldots, x_n] \mid p \text{ is } G - \text{invariant }, \deg(p) = d\}$ is a finite-dimensional vector space of which the dimension is calculated from the character table.
- Since $-1 \in G$ the space $\mathrm{Inv}_d(G) = 0$ for odd $d$.
- $(\alpha, \alpha)^d \in \mathrm{Inv}_{2d}(G)$.

# No harmonic invariants.

## Theorem.

Let $G = \mathrm{Aut}(L)$ and assume that $\langle(\alpha,\alpha)^d\rangle = \mathrm{Inv}_{2d}(G)$ for all $d = 1, \ldots, t$. Then all $G$-orbits and all non-empty layers of $L$ are spherical $2t$-designs.

## Corollary.

- If $\mathbb{R}^n$ is an irreducible $\mathbb{R}G$-module then $\mathrm{Inv}_2(G) = \langle(\alpha,\alpha)\rangle$ and $L$ is strongly eutactic.
- If additionally $\mathrm{Inv}_4(G) = \langle(\alpha,\alpha)^2\rangle$, then $L$ is strongly perfect.

# The Thompson-Smith lattice of dimension 248.

- Let $G =$Th denote the sporadic simple Thompson group.
- Then $G$ has a 248-dimensional rational representation $\rho : G \to O(248, \mathbb{Q})$.
- Since $G$ is finite, $\rho(G)$ fixes a lattice $L \leq \mathbb{Q}^{248}$.
- Modular representation theory tells us that for all primes $p$ the $\mathbb{F}_p G$-module $L/pL$ is simple.
- Therefore $L = L^{\#}$ and $L$ is even (otherwise $L_0/2L < L/2L$ would be a proper $G$-invariant submodule).
- $\mathrm{Inv}_{2d}(G) = \langle (\alpha, \alpha)^d \rangle$ for $d = 1, 2, 3$. So all layers of $L$ form spherical 6-designs and in particular $L$ is strongly perfect.
- $\min(L)\min(L^{\#}) = \min(L)^2 \geq \frac{248+2}{3} > 83.3$, so $\min(L) \geq 10$.
- There is a $v \in L$ with $(v, v) = 12$, so $\min(L) \in \{10, 12\}$.

# Strongly perfect lattices of minimum 3.

## Theorem (Venkov).

Let $L$ be an integral strongly perfect lattice of minimum 3. Then $L$ is one of

$$O_1, O_7, O_{16}, O_{22}, O_{23}.$$

$O_1 = \sqrt{3/2}\mathbb{A}_1$, $O_7 = \sqrt{2}\mathbb{E}_7^{\#}$, $O_{16} = \langle \Lambda_{16}, x \rangle$, where $\Lambda_{16}$ is the Barnes-Wall lattice in dimension 16 and $x \in \Lambda_{16}^{\#}$ satisfies $(x, x) = 3$. $O_{23}$ is the unique unimodular lattice of minimum 3 and dimension 23, $O_{22} = x^{\perp}$ for any minimal vector $x \in O_{23}$.

| $L$ | $\lvert \mathrm{Min}(L) \rvert$ | $\min(L^{\#})$ | $L^{\#}/L$ |
|---|---|---|---|
| $O_1$ | 2 | $1/3$ | 3 |
| $O_7$ | 56 | 1 | $2^6$ |
| $O_{16}$ | 512 | 2 | $2^6$ |
| $O_{22}$ | 2816 | $8/3$ | 3 |
| $O_{23}$ | 4600 | 3 | 1 |

# Strongly perfect lattices of minimum 3.

$$(D4) \quad \sum_{x\in X}(x,\alpha)^4 = \frac{3|X|m^2}{n(n+2)}(\alpha,\alpha)^2$$
$$(D2) \quad \sum_{x\in X}(x,\alpha)^2 = \frac{|X|m}{n}(\alpha,\alpha)$$

## Notation.

- Let $L \in \mathcal{L}_n$ be an integral strongly perfect lattice of minimum 3,
- $X := \mathrm{Min}(L)$, $|X| = 2s$, $Y := L_4$.
- For $\alpha \in X$ let $n_i := |\{x \in X \mid (x,\alpha) = i\}|$
- For $\beta \in Y$ let $m_i := |\{x \in X \mid (x,\beta) = i\}|$

## Identities.

- $n_i = n_{-i}$, $m_i = m_{-i}$.
- $n_i = 0$ if $i \neq 0, \pm 1, \pm 3$, $n_3 = 1$. $m_i = 0$ if $i \neq 0, \pm 1, \pm 2$.
- $s = 1 + n_1 + n_0/2$, $9 + n_1 = \frac{9s}{n}$, $81 + n_1 = \frac{3^5 s}{n(n+2)}$
- $m_1 + 4m_2 = \frac{12s}{n}$, $m_1 + 16m_2 = \frac{3^3 4^2 s}{n(n+2)}$.

# Strongly perfect lattices of minimum 3.

## Bound on dimension using $\alpha \in X$.

$n_1 = \frac{9s}{n} - 9 = \frac{3^5 s}{n(n+2)} - 81$ yields

$$\frac{25-n}{n(n+2)} s = 8$$

and hence $n \leq 24$. Moreover $n_1 = 81 \frac{n-1}{25-n}$ is integral only for $n = 1, 7, 13, 16, 17, 19, 21, 22, 23, 24$.

| $n$ | 1 | 7 | 13 | 16 | 17 | 19 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|---|---|
| $n_1$ | 0 | $3^3$ | $3^4$ | $3^3 5$ | $3^4 2$ | $3^5$ | $3^4 5$ | $3^4 7$ | $3^4 11$ | $3^4 23$ |

# Strongly perfect lattices of minimum 3.

## Bound on dimension using $\beta \in Y$.

$m_1 + 4m_2 = \frac{12s}{n}$, $m_1 + 16m_2 = \frac{3^3 4^2 s}{n(n+2)}$ allow to express $m_1$ and $m_2$ as a function in $s$ and $n$:

$$m_2 = (34 - n)\frac{s}{n(n+2)} = (34 - n)\frac{8}{25 - n}$$

Moreover $n_1|X| = m_2|Y|$: because if $(x, \beta) = 2$ then $\alpha := x - \beta \in X$ satisfies $(x, \alpha) = 1$. So

$$|Y| = 2 \cdot 3^4 \frac{n(n-1)(n+2)}{(25-n)(34-n)}$$

which is only an integer for $n = 1, 7, 16, 17, 22, 23$.

# Strongly perfect lattices of minimum 3.

## Theorem.

If $L \neq L^{\#}$, then $\min(L^{\#}) = \frac{n+2}{9}$ and $n \equiv 1 \pmod 3$.
Moreover all nonzero classes in $L^{\#}/L$ contain a vector of norm $\frac{n+2}{9}$.

Proof. Assume that $L \neq L^{\#}$ and choose $t \in L^{\#} - L$ such that

$$Q(t) = \min\{Q(t+\ell) \mid \ell \in L\}.$$

Then $|(t,x)| \leq 3/2$ for all $x \in X$ and hence $(t,x) \in \{0, \pm 1\}$. Let $p_1 := |\{x \in X \mid (t,x) = 1\}|$. Then

$$p_1 = \frac{3s}{n}(t,t) = \frac{27s}{n(n+2)}(t,t)^2 \text{ hence}$$

$$(t,t) = \frac{n+2}{9} \text{ and } p_1 = \frac{n+2}{3} \cdot \frac{s}{n} = \frac{8(n+2)^2}{3(25-n)} \in \mathbb{Z}.$$

# Strongly perfect lattices of minimum 3.

## Theorem (without proof).

The unique unimodular lattice of minimum 3 and dimension $\leq 23$ is $O_{23}$.

## Corollary.

Either $n = 1$ and $L = O_1$ or $n = 23$ and $L = O_{23}$ or $n = 7, 16, 22$, $L \neq L^{\#}$ and all nonzero classes in $L^{\#}/L$ contain a vector of norm $\frac{n+2}{9} = 1, 2, \frac{8}{3}$.

## Theorem.

If $n = 7, 16$ then $2L^{\#} \subseteq L$. If $n = 22$ then $3L^{\#} \subseteq L$.

Proof. In the first two cases $L^{\#}$ is generated by vectors of integral norm. Therefore $(t_1, t_2) \in \frac{1}{2}\mathbb{Z}$ for all $t_1, t_2 \in L^{\#}$. Similarly for $n = 22$ we obtain $(t_1, t_2) \in \frac{1}{3}\mathbb{Z}$ for all $t_1, t_2 \in L^{\#}$.

# Strongly perfect, minimum 3, $n = 7$.

For $n = 7$ we have that

$$\min(L) = 3, \min(L^{\#}) = 1, \det(L) = 2^k, 1 \leq k \leq 6, \text{ and}$$

$$\gamma(L) = \frac{3}{2^{k/7}} \leq 2^{6/7} = \gamma(\mathbb{E}_7)$$

So

$$2187 = 3^7 \leq 2^{k+6}$$

which yields $k = 6$. But then

$$\gamma(L^{\#}) = \gamma(\mathbb{E}_7)$$

implies that $L^{\#} \sim \mathbb{E}_7$ and hence $L = O_7$.

# Strongly perfect, minimum 3, $n = 22$.

## Theorem.

If $n = 22$ then $\det(L) = |L^{\#}/L| = 3$.

Proof. We know that all nonzero classes of $L^{\#}/L$ are represented by a vector $t$ with $(t, t) = \frac{8}{3}$.
For $\ell \in L$ we calculate

$$(t + \ell, t + \ell) = (t, t) + 2(t, \ell) + (\ell, \ell) \in \frac{2}{3} + \mathbb{Z}.$$

Now assume that $t_1, t_2 \in L^{\#} - L$ are such that $t_1 + t_2 \notin L$ and $t_1 - t_2 \notin L$. Then

$$4(t_1, t_2) = \underbrace{(t_1 + t_2, t_1 + t_2)}_{\in \frac{2}{3}+\mathbb{Z}} - \underbrace{(t_1 - t_2, t_1 - t_2)}_{\in \frac{2}{3}+\mathbb{Z}} \in \mathbb{Z}$$

and therefore

$$(t_1 + t_2, t_1 + t_2) = \underbrace{(t_1, t_1)}_{\in \frac{2}{3}+\mathbb{Z}} + \underbrace{2(t_1, t_2)}_{\in \mathbb{Z}} + \underbrace{(t_2, t_2)}_{\in \frac{2}{3}+\mathbb{Z}} \in \frac{1}{3} + \mathbb{Z}$$

a contradiction. Hence $|L^{\#}/L| = 3$.

# Strongly perfect, minimum 3, $n = 22$.

**Theorem.**
If $n = 22$ then $L = O_{22}$.

Proof. We know that $L^{\#} = \langle L, t \rangle$ with $(t, t) = \frac{8}{3} = \min(L^{\#})$. Let $O_1 = \langle z \rangle$, $(z, z) = 3$, $O_1^{\#} = \langle \frac{1}{3} z \rangle$. Consider

$$\Lambda := \langle L \perp O_1, t + \frac{1}{3} z \rangle \leq \mathbb{R}^{23}.$$

Then $\Lambda = \Lambda^{\#}$, $\min(\Lambda) = 3$ and hence $\Lambda \cong O_{23}$. So $L = z^{\perp} \leq O_{23}$ for some $z \in O_{23}$ of norm 3. Since $\mathrm{Aut}(O_{23})$ is transitive on $\mathrm{Min}(O_{23})$, all these lattices $z^{\perp}$ are isometric and hence $L \cong O_{22}$.

# Strongly perfect, minimum 3, $n = 16$.

## Strategy.

Let $L \in \mathcal{L}_{16}$, integral, strongly perfect, $\min(L) = 3$. Then we already have seen that $\det(L) = 2^k$, $2L^\# \subset L$.
Let $L_0 := \{\ell \in L \mid Q(\ell) \in \mathbb{Z}\}$ denote the even sublattice of $L$. Then $L_0 \leq L \leq L^\# \leq L_0^\#$, $\min(L_0) = 4$, $\mathrm{Min}(L_0) = Y$, $|L/L_0| = 2$, and $\det(L_0) = 2^{k+2}$.
We will show that $2L_0^\# \subset L_0$, and $\min(L_0^\#) \geq 2$. Moreover $\sqrt{2}L_0^\#$ is even, $\min(L_0^\#) = 2$ and from the classification of 2-elementary 16-dimensional even lattices by Scharlau and Venkov, $L_0 \cong \mathrm{BW}_{16}$ is the Barnes-Wall lattice.
Then $L = \langle L_0, x\rangle$ for any vector $x \in L_0^\#$ of norm $(x, x) = 3$. Again $\mathrm{Aut}(\mathrm{BW}_{16})$ is transitive on the vectors of norm 3 in the dual lattice, so $L$ is uniquely determined.

# Strongly perfect, minimum 3, $n = 16$.

Choose $\xi \in L_0^\# - L^\#$ minimal in $\xi + L$.
Then $(\xi, x) \in \frac{1}{2} + \mathbb{Z}$ for all $x \in X$ and $|(\xi, x)| \leq \frac{3}{2}$ so $(\xi, x) \in \{\pm\frac{1}{2}, \pm\frac{3}{2}\}$.
Let $o_i := |\{x \in X \mid (\xi, x) = \frac{i}{2}\}|$ for $i = 1, 3$. Then

$$\begin{aligned} o_1 + o_3 &= s = 256 \\ o_1 + 9o_3 &= 2^2 3 (\xi,\xi) \tfrac{s}{n} = 192(\xi,\xi) \\ o_1 + 3^4 o_3 &= 2^4 3^3 (\xi,\xi)^2 \tfrac{s}{n(n+2)} = 384(\xi,\xi)^2 \end{aligned}$$

yields $(\xi,\xi)^2 - 5(\xi,\xi) + 6 = 0$, so $(\xi,\xi) \in \{2, 3\}$. In particular all elements in $L_0^\#$ have integral norms and therefore $2L_0^\# \subset L_0$.

# The Barnes-Wall lattices of dimension $2^d$.

- Let $d \in \mathbb{N}$, $m := \lfloor \frac{d}{2} \rfloor$, $A := \mathbb{F}_2^d$ and $(e_a \mid a \in A)$ an orthogonal basis of $\mathbb{R}^{2^d}$ with $(e_a, e_a) = 2^{-m}$.
- For an affine subspace $X = a + U$, $a \in A$, $U \leq A$ let $\chi_X := \sum_{x \in X} e_x \in \mathbb{R}^{2^d}$.
- Then $(\chi_X, \chi_X) = 2^{-m}|X| = 2^{k-m}$, where $k = \dim(X) := \dim(U)$.
- Let $\mathcal{A}(d, k)$ denote the set of all affine subspaces of $A$ of dimension $k$.
- For $X \in \mathcal{A}(d, 2k)$ the norm $(\chi_X, \chi_X) = 2^{2k-m}$.
- Define the Barnes-Wall lattice

$$\mathrm{BW}_d := \langle 2^{m-k} \chi_X \mid k = 0, \ldots, m, X \in \mathcal{A}(d, 2k) \rangle_{\mathbb{Z}}.$$

# The Barnes-Wall lattices of dimension $2^d$.

## Some properties of $\mathrm{BW}_d$.

- $\min(\mathrm{BW}_d) = 2^m$, where $m = \lfloor \frac{d}{2} \rfloor$, $\det(\mathrm{BW}_d) = \begin{cases} 2^m & d \text{ even} \\ 1 & d \text{ odd} \end{cases}$.
- $\mathrm{BW}_1 = \mathbb{Z}^2$, $\mathrm{BW}_2 = \mathbb{D}_4$, $\mathrm{BW}_3 = \mathbb{E}_8$.
- $$\mathrm{Min}(\mathrm{BW}_d) = \dot{\cup}_{k=0}^{m} \dot{\cup}_{X \in \mathcal{A}(d,2k)} S(X)$$
  where $S(X)$ are those minimal vectors in $\mathrm{BW}_d$ that are obtained from $2^{m-k}\chi_X$ by changing certain $e_a$ to $-e_a$.
- It holds that $|S(X)| = 2^{1+2k+(2k-1)k}$ for $\dim(X) = 2k$.
- In particular $s_d := |\mathrm{Min}(\mathrm{BW}_d)| = \sum_{k=0}^{m} |\mathcal{A}(d,2k)| 2^{1+2k+(2k-1)k} =$

$$\sum_{k=0}^{m} \binom{d}{2k}_2 2^{d-2k} 2^{1+2k+(2k-1)k} = 2^{d+1} \sum_{k=0}^{m} 2^{(2k-1)k} \binom{d}{2k}_2$$

where $\binom{d}{\ell}_2 = \frac{(2^d-1)\ldots(2^{d-\ell+1}-1)}{(2^\ell-1)\ldots(2-1)}$ is the number of $\ell$-dimensional subspaces of $\mathbb{F}_2^d$.

# The Barnes-Wall lattices of dimension $2^d$.

## Theorem (Sidelnikov, Venkov).

For $d \geq 3$ the set $\mathrm{Min}(\mathrm{BW}_d)$ is a spherical 7-design.

Proof. We have to show that

$$\sum_{x,y \in \mathrm{Min}(\mathrm{BW}_d)} (x,y)^6 = \frac{1 \cdot 3 \cdot 5}{2^d(2^d+2)(2^d+4)} 2^{6m} |\mathrm{Min}(\mathrm{BW}_d)|^2$$

Since $\mathrm{Aut}(\mathrm{BW}_d)$ is transitive on $\mathrm{Min}(\mathrm{BW}_d)$ it suffices to show that for $y := 2^m e_0 \in \mathrm{Min}(\mathrm{BW}_d)$

$$\sum_{x \in \mathrm{Min}(\mathrm{BW}_d)} (x,y)^6 = \frac{1 \cdot 3 \cdot 5}{2^d(2^d+2)(2^d+4)} 2^{6m} |\mathrm{Min}(\mathrm{BW}_d)|.$$

Then for any $X \in \mathcal{A}(d, 2k)$ and any $v \in S(X)$ we have $(v,y) = 0$ if $X$ is not a subspace of $\mathbb{F}_2^d$ (so $0 \notin X$) and

$$(v,y)^2 = (2^{m-k}\chi_X, 2^m e_0)^2 = (2^{2m-k}(e_0,e_0))^2 = 2^{2m-2k}.$$

Therefore $\sum_{x \in S(X)} (x,y)^{2p} = 2^{1+2k+(2k-1)k} 2^{2p(m-k)}$ if $X \leq \mathbb{F}_2^d$ is a $2k$-dimensional subspace and 0 otherwise.

# $\mathrm{Min}(\mathrm{BW}_d)$ is a 6-design.

So in total $\sum_{x\in \mathrm{Min}(\mathrm{BW}_d)}(x,y)^{2p} = \sum_{X\leq \mathbb{F}_2^d}\sum_{x\in S(X)}(x,y)^{2p} =$

$$\sum_{k=0}^{m} 2^{1+2k+(2k-1)k} 2^{2p(m-k)} \binom{d}{2k}_2 = 2^{2pm+1}\sum_{k=0}^{m} 2^{(2k-1)k}\binom{d}{2k}_2 \left(\frac{1}{2}\right)^{2k(p-1)}$$

$= 2^{2pm+1} h_d(1/2^{p-1})$ where $h_d(z) = \sum_{k=0}^{m} 2^{(2k-1)k}\binom{d}{2k}_2 z^{2k} \in \mathbb{Z}[z]$.

We introduce $g_d(z) = \sum_{\ell=0}^{d} 2^{\ell(\ell-1)/2}\binom{d}{\ell}_2 z^{\ell} \in \mathbb{Z}[z]$ so that $2h_d(z) = g_d(z) + g_d(-z)$.

## Lemma.

$g_d(z) = (1+z)(1+2z)\ldots(1+2^{d-1}z)$ for all $d \geq 1$.

In particular $g_d(-1/2^2) = 0$ for $d \geq 3$ and $g_d(-1) = 0$ so $\sum_{x\in \mathrm{Min}(\mathrm{BW}_d)}(x,y)^6 = 2^{6m} g_d(1/4)$ and

$$|\,\mathrm{Min}(\mathrm{BW}_d)| = 2^{d+1}\sum_{k=0}^{m} 2^{(2k-1)k}\binom{d}{2k}_2 = 2^d(2h_d(1)) = 2^d g_d(1).$$

# $\mathrm{Min}(\mathrm{BW}_d)$ is a 6-design.

$$\sum_{x \in \mathrm{Min}(\mathrm{BW}_d)} (x,y)^6 = 2^{6m} g_d(1/4) = 2^{6m}(1+\frac{1}{2^2})(1+\frac{2}{2^2})\ldots(1+\frac{2^{d-1}}{2^2})$$

$$= 2^{6m}\frac{5\cdot 3}{2^2\cdot 2}(1+1)\ldots(1+2^{d-3})$$

$$= 2^{6m}\frac{5\cdot 3}{2(2^{d-1}+1)2^2(2^{d-2}+1)}(1+1)\ldots(1+2^{d-3})(1+2^{d-2})(1+2^{d-1})$$

$$= \frac{2^{6m}\cdot 1\cdot 3\cdot 5\cdot 2^d g_d(1)}{2^d(2^d+2)(2^d+4)}$$

Since $2^d g_d(1) = |\,\mathrm{Min}(\mathrm{BW}_d)|$ and $2^d = \dim(\mathrm{BW}(d))$, $2^m = \min(\mathrm{BW}_d)$ this is what we needed to show.

# Proof of Lemma.

## Lemma.

$g_d(z) = (1+z)(1+2z)\dots(1+2^{d-1}z)$ for all $d \geq 1$.

Proof.

$$g_d(z) = \sum_{\ell=0}^{d} 2^{\ell(\ell-1)/2} \binom{d}{\ell}_2 z^\ell \text{ with } \binom{d}{\ell}_2 = \frac{(2^d-1)\dots(2^{d-\ell+1}-1)}{(2^\ell-1)\dots(2-1)}$$

Clearly $g_1(z) = 1+z$ and $\binom{d+1}{\ell}_2 = \binom{d}{\ell}_2 + 2^{d-\ell+1}\binom{d}{\ell-1}_2$ so

$$g_{d+1}(z) = g_d(z) + \sum_{\ell=0}^{d} 2^{\ell(\ell-1)/2} 2^{d-\ell+1} \binom{d}{\ell-1}_2 z^\ell$$

$$= g_d(z) + 2^d \sum_{\ell=1}^{d} 2^{\ell(\ell-1)/2} 2^{1-\ell} \binom{d}{\ell-1}_2 z^\ell$$

$$= g_d(z) + 2^d z \sum_{\ell=0}^{d-1} 2^{\ell(\ell-1)/2} \binom{d}{\ell}_2 z^\ell = (1+2^d z) g_d(z).$$