Codes and invariant theory.

Gabriele Nebe
Lehrstuhl D für Mathematik, RWTH Aachen, 52056 Aachen, Germany,
nebe@math.rwth-aachen.de

1 Summary.

There is a beautiful analogy between most of the notions for lattices and codes and it seems to be quite promising to develop coding theory analogues of concepts known in the theory of lattices and modular forms and vice versa. Some of these analogies are presented in this short note.

2 Lattices.

2.1 Lattices and modular forms.

A lattice L is a discrete cocompact subgroup of euclidean space $(\mathbb{R}^N, (,))$ or equivalently the set of all integral linear combinations of a basis of $\mathbb{R}^N$. One measure for the quality of a lattice is the density of the associated sphere packing. The diameter of the spheres is the minimal distance between two distinct lattice points which is also the square root of the *minimum* of L,

$$\min(L) = \min\{(\ell,\ell) \mid \ell \in L,\ \ell \neq 0\}.$$

The theta-series of L is the generating function of the norms of the elements in L

$$\vartheta_L := \sum_{\ell \in L} q^{(\ell,\ell)} = 1 + a_{\min(L)} q^{\min(L)} + \dots$$

where $a_n := |\{\ell \in L \mid (\ell,\ell) = n\}|$. If one substitutes $q = \exp(\pi i z)$ with $\Im(z) > 0$ then this theta series becomes a holomorphic function on the upper half plane. It also satisfies certain additional invariance properties under a discrete group of Möbius transformations.

The most famous example here is the one of *unimodular* lattices. A lattice L is called *unimodular*, if it coincides with its *dual lattice*

$$L^{\#} = \{v \in \mathbb{R}^N \mid (v, L) \subset \mathbb{Z}\}$$

In this case $(\ell,\ell) \in \mathbb{Z}$ for all $\ell \in L$ and hence ϑ_L is invariant under the translation $z \mapsto z+2$. By Poisson summation the theta-series of the dual lattice is

$$\vartheta_{L^{\#}}(z) = (\frac{z}{i})^{-N/2} \sqrt{\det(L)}\, \vartheta_L(-\frac{1}{z})$$

which shows that the theta-series of a unimodular lattice is a modular form for the theta group

$$\Theta := \langle z \mapsto z+2, z \mapsto \frac{-1}{z} \rangle$$

of weight $\frac{N}{2}$.

The ring of modular forms is a finitely generated graded ring. For the theta group this ring is

$$\mathcal{M}(\Theta) = \oplus_{N=0}^{\infty} \mathcal{M}_{N/2}(\Theta) = \mathbb{C}[\vartheta_{\mathbb{Z}}, \vartheta_{E_8}]$$

where $\mathbb{Z}$ is the 1-dimensional standard-lattice and E_8 the unique unimodular lattice of dimension 8 with minimum 2. Equivalently this ring is the polynomial ring in

$$\vartheta_{\mathbb{Z}} = 1 + 2\sum_{a=1}^{\infty} q^{a^2} \text{ and } \Delta_8 = \frac{1}{16}(\vartheta_{\mathbb{Z}}^8 - \vartheta_{E_8}) = q(\prod_{a=1}^{\infty}(1-q^{2a-1})(1-q^{4a}))^8.$$

A closer inspection of the space of such modular forms of weight $N/2$ allows to deduce the following upper bound on the minimum of a unimodular lattice.

Theorem 1. *If L is a unimodular lattice of dimension N, then* $\min(L) \leq 1 + \lfloor \frac{N}{8} \rfloor$.

2.2 Shadows.

The bound in Theorem 1 can be significantly improved by using the concept of the shadow of a lattice: Let L be a unimodular lattice. Then the set

$$S(L) = \{v \in \mathbb{R}^N \mid 2(\ell, v) \equiv (\ell, \ell) \pmod 2 \text{ for all } \ell \in L\}$$

is called the *shadow* of L. If L is *even*, i.e. $(\ell, \ell) \in 2\mathbb{Z}$ for all $\ell \in L$, then $S(L) = L$. Otherwise the *even sublattice*

$$L_{ev} := \{\ell \in L \mid (\ell, \ell) \in 2\mathbb{Z}\}$$

is a sublattice of index 2 in L and

$$S(L) = L_{ev}^{\#} \setminus L$$

is the nontrivial coset of L contained in $L_{ev}^{\#}$. In both cases the theta series of $S(L)$ may be obtained from the one of L by a variable transformation:

$$\vartheta_{S(L)}(z) = (\frac{z}{i})^{-N/2} \vartheta_L(1 - \frac{1}{z}).$$

Since $\vartheta_{S(L)}$ is the generating function of the norms of the elements in the shadow, its q-expansion has non-negative integral coefficients. This observation allows to improve Theorem 1 (see [12]).

Theorem 2. *If L is a unimodular lattice of dimension N, then* $\min(L) \leq 2 + 2\lfloor \frac{N}{24} \rfloor$ *unless $N = 23$ when the bound is* 3.

2.3 Harmonic theta series.

One possibility to encode more information about the lattice in its theta series is to consider harmonic polynomials $P \in \mathbb{C}[X_1, \ldots, X_N]$ which are homogeneous of degree d. Then

$$\vartheta_{P,L}(z) = \sum_{\ell \in L} P(\ell) q^{(\ell,\ell)}$$

is a modular form of weight $d + N/2$. For $d > 0$ the constant term $P(0) = 0$ and hence the q-expansion of $\vartheta_{P,L}$ starts with $a_{\min(L),P} q^{\min(L)}$ where for $n \in \mathbb{N}$

$$a_{n,P} = \sum_{\ell \in L, (\ell,\ell)=n} P(\ell)$$

is the sum over the n-th layer of the lattice L. This observation sometimes allows to show that for small degree $d > 0$ and large minimum, the harmonic theta series $\vartheta_{P,L}$ vanishes, hence $a_{n,P} = 0$ for all n and all non-constant harmonic polynomials P of degree $\leq d$ which means that all layers of L form spherical d-designs. For instance all layers of an even unimodular lattice $L \leq \mathbb{R}^N$ of minimum $\min(L) = 2 + N/12$ are spherical 11-designs. The philosophy to use designs to analyze and construct good lattices was introduced by Boris Venkov (see [15], [3] and [11] for its use in combination with shadow theory).

2.4 Siegel theta series and the Φ-operator.

Another way to obtain more information about the lattice is to consider higher genus theta series

$$\vartheta_L^{(m)}(Z) := \sum_{(\ell_1,\ldots,\ell_m) \in L^m} \exp(\pi i \operatorname{Trace}(((\ell_k, \ell_j))Z)$$

which is a holomorphic function on the Siegel upper half plane

$$\mathcal{H}_m := \{Z = X + iY \in \mathbb{C}_{sym}^{m \times m} \mid Y \text{ positive definite } \}.$$

If L is a unimodular lattice of dimension N, then $\vartheta_L^{(m)}$ is a modular form for $\Theta^{(m)} \leq \mathrm{Sp}_{2m}(\mathbb{Z})$ of weight $N/2$. One hence gets a whole series $\Theta^{(1)} := \Theta, \Theta^{(2)}, \ldots$ of modular groups of which the rings of modular forms can be used to deduce properties of unimodular lattices. Their rings of modular forms are connected by the *Siegel* Φ*-operator*. This a surjective linear operator

$$\Phi : \mathcal{M}(\Theta^{(m)}) \to \mathcal{M}(\Theta^{(m-1)})$$

that respects the weight. It maps $\vartheta_L^{(m)}$ to $\vartheta_L^{(m-1)}$ and gives a filtration of the space of modular forms for $\Theta^{(m)}$ of a given weight by the kernels of the powers of Φ which may be turned into an orthogonal decomposition using the Petersson scalar product on $\mathcal{M}(\Theta^{(m)})$. Hence

$$\mathcal{M}(\Theta^{(m)}) = \ker(\Phi) \perp \ker(\Phi)^\perp \text{ and } \ker(\Phi)^\perp \cong \Phi(\mathcal{M}(\Theta^{(m)})) = \mathcal{M}(\Theta^{(m-1)})$$

so the Φ-operator inductively reduces the investigation of $\mathcal{M}(\Theta^{(m)})$ to the one of $\ker(\Phi)$.

2.5 Hecke operators.

Hecke operators are linear operators acting on the graded components of rings of modular forms. They commute with the Φ-operator and respect the filtration above. For unimodular lattices there is a nice construction of Hecke operators using the Kneser neighboring concept ([5]) which is introduced in [10].

For a prime p two unimodular lattices L and M are called p-neighbors, if they intersect in a sublattice of index p, $[L : L \cap M] = [M : L \cap M] = p$. Then the Hecke operator K_p maps the theta series of a lattice L to the sum over the theta series of its p-neighbors. The operators K_p commute for all primes p. Their common eigenforms provide interesting examples of Siegel cusp forms.

3 Codes

3.1 Codes and invariant rings.

For a finite ring R and a finite left R-module V (the alphabet) a linear code of length N is an R-submodule $C \leq V^N$. For a nonsingular biadditive form $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ the *dual code* is

$$C^\perp := \{v \in V^N \mid \sum_{i=1}^{N} \beta(v_i, c_i) = 0 \text{ for all } c \in C\}.$$

C is called *self-dual*, if $C = C^\perp$. The most famous examples are linear binary codes, where $V = R = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and $\beta(x, y) := \frac{1}{2}xy$.

For a letter $v \in V$ and a word $c \in V^N$ let $a_v(c) := |\{i \in \{1, \ldots, N\} \mid c_i = v\}|$ count the number of occurrences of v in c. The error-correcting properties of C are measured by its minimal Hamming-distance

$$d(C) := \min\{N - a_0(c) \mid c \in C, c \neq 0\}.$$

This may be read off from the *complete-weight-enumerator*

$$\mathrm{cwe}_C := \sum_{c \in C} \prod_{v \in V} x_v^{a_v(c)} \in \mathbb{C}[x_v \mid v \in V]_N$$

the generating function of the weight distributions a_v which is a complex homogeneous polynomial of degree N in $|V|$ variables.

If C is a code, then cwe_C is invariant under the variable substitution $x_v \mapsto x_{rv}$ for all $r \in R^*$. If $C = C^\perp$ then also $\mathrm{cwe}_C = \mathrm{cwe}_{C^\perp}$, where the weight enumerator of the dual code is obtained by substituting the variable x_v by $\sum_{w \in V} \exp(2\pi i \beta(v, w)) x_w$ and dividing by $|C|$. For a self-dual binary code C, the exponents $a_1(c)$ and $a_0(c)$ are even for all $c \in C$. Therefore cwe_C is invariant under the group

$$D_{16} = \langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle.$$

This point of view was introduced by Gleason in 1970. The invariant ring of D_{16} is a polynomial ring

$$\mathrm{Inv}(D_{16}) = \mathbb{C}[\mathrm{cwe}_{i_2}, \mathrm{cwe}_{e_8}]$$

where one may choose the generators

$$\mathrm{cwe}_{i_2} = x_0^2 + x_1^2 \text{ and } \delta_8 = \frac{1}{4}(\mathrm{cwe}_{i_2}^4 - \mathrm{cwe}_{e_8}) = (x_0x_1(x_0 - x_1)(x_0 + x_1))^2.$$

As for lattices this allows to show that

Theorem 3. *If C is a self-dual binary code of length N, then $d(C) \leq 2 + 2\lfloor \frac{N}{8} \rfloor$.*

Gleason gave analogous results for other Types of self-dual codes over finite fields and further analogues of this theorem were proven during the past 30 years. In [9], we develop a unifying theory that gives an explicit construction of a finite matrix group $\mathcal{C} \leq \mathrm{GL}_{|V|}(\mathbb{C})$, the associated Clifford-Weil group, such that the complete weight enumerators of self-dual codes of a given Type are invariant under $\mathcal{C}$. For a quite general class of rings, including matrix rings over finite fields and Galois rings, we can prove that, conversely, the invariant ring of the associated Clifford-Weil group is spanned by the complete weight enumerators of self-dual codes. As for binary codes this allows to use the invariant theory of $\mathcal{C}$ to bound the minimal distance of more general self-dual codes.

3.2 Shadows.

There is also a notion of shadow for self-dual codes of a given Type (see [9, Section 1.12]) which has been quite fruitfully used to improve the bounds on the minimal weight of a code. For a binary self-dual code $C = C^\perp \leq \mathbb{F}_2^N$, the shadow

$$S(C) = \{v \in \mathbb{F}_2^N \mid 2\sum_{i=1}^{N} v_i c_i \equiv \sum_{i=1}^{N} c_i^2 \pmod 4 \text{ for all } c \in C\}.$$

The weight enumerator of $S(C)$ may be obtained from the one of C by replacing x_0 by $\frac{1}{\sqrt{2}}(x_0 + x_1)$ and x_1 by $\frac{i}{\sqrt{2}}(x_0 - x_1)$. Since $\mathrm{cwe}_{S(C)}$ again has non-negative (integral) coefficients this allows to improve the bounds in Theorem 3:

Theorem 4. *(see [13]) If C is a self-dual binary code of length N, then $d(C) \leq 4+4\lfloor \frac{N}{24} \rfloor$ unless $N \equiv 22 \pmod{24}$ when the bound is $6 + 4\lfloor \frac{N}{24} \rfloor$.*

3.3 Harmonic weight-enumerators.

Replacing the representation theory of the orthogonal group by the one of the symmetric group, the concept of spherical designs finds its analogue in the combinatorial block designs. In this spirit [1] and [2] define harmonic weight enumerators of linear self-dual codes over finite fields. These are relative invariants of the associated Clifford-Weil group. They often reveal enough information on the codes to classify self-dual codes of small length and with high minimal distance and on the other hand also show that such codes yield good block designs.

3.4 Higher weight-enumerators and the finite Φ-operator.

Also for codes it is sometimes useful to consider more than one codeword at a time. An m-tuple $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in C^m$ of codewords may be viewed as a codeword $\underline{c} \in (V^m)^N$. Then for a given self-dual code $C \leq V^N$ the code

$$C(m) := \{\underline{c} \in C^m\} \leq (V^m)^N$$

is a self-dual $R^{m\times m}$-linear code over the alphabet V^m. The degree m weight-enumerator of C is

$$\mathrm{cwe}_C^{(m)} := \mathrm{cwe}_{C(m)} = \sum_{\underline{c}\in C^m} \prod_{v\in V^m} x_v^{a_v(\underline{c})} \in \mathbb{C}[x_v \mid v \in V^m]$$

and the associated Clifford-Weil group $\mathcal{C}_m$ may be obtained by replacing R by the matrix ring $R^{m\times m}$, V by V^m and changing β accordingly. This is the main reason, why we need to include non-commutative rings in our theory. Even for binary codes the matrix ring $\mathbb{F}_2^{m\times m}$ naturally occurs as a ground ring when considering degree m weight-enumerators. In particular our theorem implies that the degree m weight-enumerators of binary self-dual codes span the invariant ring of $\mathcal{C}_m = 2_+^{1+2m}.O_{2m}^+(2) \leq \mathrm{GL}_{2^m}(\mathbb{C})$.

The Φ-operator for codes was introduced by B. Runge [14]. It maps $\mathrm{cwe}_C^{(m)}$ to $\mathrm{cwe}_C^{(m-1)}$ and hence defines a surjective linear operator

$$\Phi : \mathrm{Inv}(\mathcal{C}_m) \to \mathrm{Inv}(\mathcal{C}_{m-1}).$$

As for modular forms one obtains a filtration

$$\mathrm{Inv}_N(\mathcal{C}_m) \supseteq \ker(\Phi^m) \supseteq \ker(\Phi^{m-1}) \supseteq \ldots \supseteq \ker(\Phi) \supseteq \{0\} \quad (\star)$$

and the associated orthogonal decomposition with respect to the natural $\mathcal{C}_m$-invariant Hermitian scalar product on $\mathrm{Inv}_N(\mathcal{C}_m)$. In [7] it is shown that for the classical Types of codes over finite fields this decomposition is the eigenspace decomposition of the Kneser-Hecke-operator defined in the next section.

3.5 Kneser-Hecke-operators.

[7] translates the construction in [10] of Hecke operators to self-dual codes over finite fields. Two self-dual codes $C, D \leq \mathbb{F}^N$ over a finite field $\mathbb{F}$ are called *neighbors*, if $C \cap D$ has codimension 1 in C and in D. Then the Kneser-Hecke-operator T is the self-adjoint linear operator on $\mathrm{Inv}_N(\mathcal{C}_m)$ mapping $\mathrm{cwe}_C^{(m)}$ to the sum $\sum_D \mathrm{cwe}_D^{(m)}$ of the degree m weight-enumerators of all neighbors of C. In contrast to the lattice case, the eigenvalues of T may be given a priori and one may show that the eigenspace decomposition of T is the one associated to the filtration $(\star)$ above.

In the lattice case, Hecke operators have an interpretation as sums of double cosets of the modular group. For codes, the preprint [8] uses the fact that $\mathcal{C}_m$ is a finite Weil-representation to obtain T as a sum of $\mathcal{C}_m$ double cosets.

References

[1] C. Bachoc, On harmonic weight enumerators of binary codes, *Designs, Codes, and Cryptography* **18** (1999), 11–28

[2] C. Bachoc, Harmonic weight enumerators of non-binary codes and MacWilliams identities, in *Codes and association schemes (Piscataway, NJ, 1999)*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., **56**, Amer. Math. Soc., Providence, RI, 2001; pp. 1–23

[3] C. Bachoc, B. Venkov, Modular forms, lattices and spherical designs. In [6] 87-112.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1998, 3rd. ed. 1998.

[5] M. Kneser, Klassenzahlen definiter quadratischer Formen, *Archiv der Math.* **8** (1957), 241-250.

[6] J. Martinet (editor) *Réseaux euclidiens, designs sphériques et formes modulaires.* L'Ens. Math. Monographie **37** (2001)

[7] G. Nebe, An analogue of Hecke-operators in coding theory. Preprint (2005)

[8] G. Nebe, Finite Weil-representations and associated Hecke-algebras. Preprint (2006).

[9] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-dual codes and invariant theory.* Springer-Verlag (2006).

[10] G. Nebe and B. B. Venkov, On Siegel modular forms of weight 12, *J. Reine Angew. Math.* **531** (2001) 49–60.

[11] G. Nebe and B. B. Venkov, Unimodular lattices with long shadow. *J. Number Theory* **99** (2003) 307-317

[12] E. M. Rains and N. J. A. Sloane, The shadow theory of modular and unimodular lattices. J. Number Th. **73** (1998), 359-389.

[13] E. M. Rains, Shadow bounds for self-dual codes. IEEE Trans. Inform. Theory **44** (1998) 134–139.

[14] B. Runge, Codes and Siegel modular forms, *Discrete Math.* **148** (1996) 175–204.

[15] B. Venkov, Réseaux et designs sphériques. in [6] 10-86.