

# Octonions, Cubes, Embeddings

Martin H. Weissman

March 2, 2009

Let  $k$  be a field, with  $\text{char}(k) \neq 2$ . A **Hurwitz algebra** over  $k$  is a finite-dimensional, unital,  $k$ -algebra  $A$ , together with a quadratic form  $N: A \rightarrow k$ , such that the associated bilinear form is nondegenerate and:

$$N(xy) = N(x)N(y), \text{ for all } x, y \in A.$$

Every Hurwitz algebra over  $k$  has dimension 1, 2, 4, or 8, as a  $k$  vector space. An 8-dimensional Hurwitz  $k$ -algebra is often called a **Cayley** or **octonion** algebra.

The isomorphism class of a Cayley  $k$ -algebra  $A$  is determined by the isomorphism class of the quadratic space  $(A, N)$ . The quadratic form  $N$  of a Cayley  $k$ -algebra is always a Pfister form. Every Pfister form of dimension 8 is hyperbolic or anisotropic. There are no anisotropic forms over  $\mathbb{Q}_p$  of dimension greater than 4. There are two dimension 8 Pfister forms over  $\mathbb{R}$ . The isomorphism class of a quadratic form over  $\mathbb{Q}$  is determined by local invariants. There is no local-global obstruction for Cayley algebras.

Constructing all Cayley algebras (up to isomorphism) over  $\mathbb{Q}$  (or a local field) is not difficult. One construction is the Cayley-Dickson process: begin with a quaternion algebra  $B$  over  $\mathbb{Q}$ . Define  $\mathbb{O} = B \oplus B$  as a  $\mathbb{Q}$ -vector space. Define a  $\mathbb{Q}$ -algebra structure on  $\mathbb{O}$  by:

$$(u, v) \cdot (z, w) = (uz - \bar{w}v, wu + v\bar{z}).$$

Define the main involution on  $\mathbb{O}$  by  $\overline{(u, v)} = (\bar{u}, -v)$ .

NOTE: Status update: The Cayley-Dickson construction is implemented in SAGE by J. Hanke and M. Weissman.

A common construction of a “nonsplit” octonion algebra over  $\mathbb{Q}$  arises as follows: Let  $\mathbf{P}^2(\mathbb{F}_2)$  denote the projective space of lines in  $\mathbb{F}_2^3$  (a set with seven elements). Since  $\mathbb{F}_2$  has one nonzero element, there is a natural bijection

$$\mathbf{P}^2(\mathbb{F}_2) \leftrightarrow \mathbb{F}_2^3 - \{0\}.$$

Define  $\mathbb{O}$  to be the  $\mathbb{Q}$ -vector space whose basis is the set  $\{1\} \cup \mathbf{P}^2(\mathbb{F}_2)$ . If  $\vec{x} \in \mathbf{P}^2(\mathbb{F}_2)$ , write  $e_{\vec{x}}$  for the associated basis element of  $\mathbb{O}$ . Define a function  $f: \mathbf{P}^2(\mathbb{F}_2) \times \mathbf{P}^2(\mathbb{F}_2) \rightarrow \mathbb{F}_2$  by:

$$f(\vec{x}, \vec{y}) = \sum_{\sigma \in A_3} x_{\sigma(1)}y_{\sigma(1)} + x_{\sigma(1)}y_{\sigma(2)} + y_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)}.$$

Define a  $\mathbb{Q}$ -algebra structure on  $\mathbb{O}$  by identifying 1 as the unit, and defining:

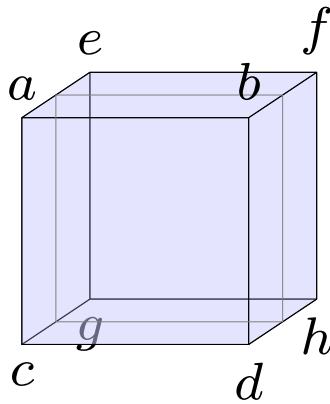
$$(e_{\vec{x}}) \cdot (e_{\vec{y}}) = e_{\vec{x}+\vec{y}} \cdot (-1)^{f(\vec{x},\vec{y})}.$$

The main involution on  $\mathbb{O}$  is determined by  $\bar{1} = 1$  and  $\overline{e_{\vec{x}}} = -e_{\vec{x}}$ .

CUBES

The following results are due to Manjul Bhargava. Define a **Bhargava cube** to be an element

$$C \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2.$$



Slicing the above cube along the light line yields the two matrices:

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

$$N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

The group  $SL_2(\mathbb{Z})^3$  acts on the  $\mathbb{Z}$ -module of Bhargava cubes, via the tensor cube of the standard action of  $SL_2(\mathbb{Z})$  on  $\mathbb{Z}^2$ . There is a unique (up to normalization) quartic polynomial invariant for the resulting geometric action; its (normalized) value is called the **discriminant**, and denoted  $\Delta(C)$ .

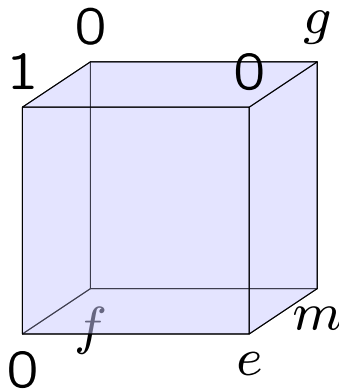
From a Bhargava cube  $C$ , one may construct three ordered pairs of matrices by slicing:

$$C: (M_1, N_1) \text{ or } (M_2, N_2) \text{ or } (M_3, N_3).$$

These yields three integer-valued quadratic forms, all of the same discriminant  $\Delta(C)$ :

$$Q_i(x, y) = -\det(M_i x - N_i y), \text{ for } i = 1, 2, 3.$$

The cube  $C$  is called **projective** if the three associated quadratic forms  $Q_1, Q_2, Q_3$  are primitive. Projective cubes can be brought, by the action of  $SL_2(\mathbb{Z})^3$ , into a “normal form” as displayed in the margin.



The three resulting quadratic forms, all of discriminant  $\Delta = m^2 + 4efg$ , are:

$$Q_1(x, y) = -ex^2 + mxy + fgy^2,$$

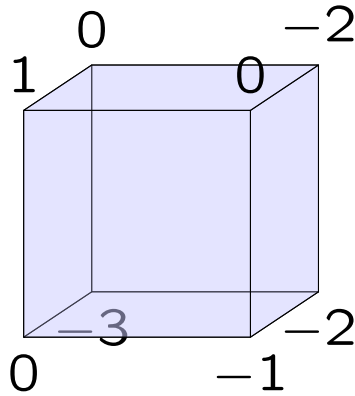
$$Q_2(x, y) = -fx^2 + mxy + egy^2,$$

$$Q_3(x, y) = -gx^2 + mxy + efy^2.$$

The following theorem is the starting point for Bhargava's work:

**Theorem 1 (Bhargava)** *Fix an integer  $\Delta$ . The orbits of  $SL_2(\mathbb{Z})^3$  on the set of projective Bhargava cubes of discriminant  $\Delta$  are in one-to-one correspondence with the set of triples  $([Q_1], [Q_2], [Q_3])$  of  $SL_2(\mathbb{Z})$ -equivalence classes of primitive binary quadratic forms of discriminant  $\Delta$ , such that  $[Q_1] \circ [Q_2] \circ [Q_3] = [1]$ , in the sense of Gauss composition.*

The significance of Bhargava's theorem is that it provides a completely new definition of Gauss composition. Indeed, in any group  $G$ , knowledge of the set of triples  $(g_1, g_2, g_3)$  such that  $g_1 \circ g_2 \circ g_3 = 1$  suffices to determine the group law. In practice, it implies that, given two primitive quadratic forms  $Q_1, Q_2$ , there exists a projective Bhargava cube  $C$  in normal form, from which  $Q_3$  can be easily computed.



For example, consider the following two quadratic forms of discriminant  $-20$ :

$$Q_1(x, y) = x^2 + 5y^2 \sim x^2 - 2xy + 6y^2.$$

$$Q_2(x, y) = 3x^2 - 2xy + 2y^2.$$

These fit into the cube above. The third quadratic form is:

$$Q_3(x, y) = 2x^2 - 2xy + 3y^2.$$

Since  $Q_3 \sim Q_2$ ,  $[Q_2] \cdot [Q_2] = [1]$  in the class group.

Orders

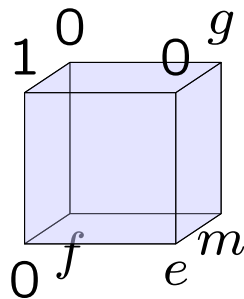
Let  $\mathbb{O}$  denote the nonsplit octonion algebra over  $\mathbb{Q}$ , with basis  $\{1\} \cup \mathbf{P}^2(\mathbb{F}_2)$ . We are interested in writing down a maximal order in  $\mathbb{O}$ . The **naive guess**  $\Omega_{ng} = \mathbb{Z} \oplus \bigoplus_{\vec{x} \in \mathbf{P}^2(\mathbb{F}_2)} \mathbb{Z}e_{\vec{x}}$  at a maximal order in  $\mathbb{O}$  is incorrect! The correct maximal order was identified by Coxeter, after many mistaken attempts (e.g. by Kirmse). There exists a maximal order  $\Omega$ , which contains  $\Omega_{ng}$  with index 16; Coxeter describes this order explicitly.

The following statements characterize the order  $\Omega$  as a lattice containing  $\Omega_{ng}$ : if  $\vec{x} + \vec{y} = \vec{z}$ , in  $\mathbf{P}^2(\mathbb{F}_2)$ , then the octonion  $1/2 \cdot (\pm 1 \pm e_{\vec{x}} \pm e_{\vec{y}} \pm e_{\vec{z}})$  is in  $\Omega$ . Furthermore,  $\Omega$  contains an element  $\omega = 1/2 \cdot (e_{\vec{x}} + e_{\vec{y}} + e_{\vec{z}} + e_{\vec{w}})$ , for some  $\vec{x}, \vec{y}, \vec{z}, \vec{w} \in \mathbf{P}^2(\mathbb{F}_2)$ , such that  $N(\omega) = 1$ .

The maximal order  $\Omega$  is isometric to the  $E_8$  root lattice. The theta function of the  $E_8$  root lattice is just the Eisenstein series  $E_4$  (of weight 4, level 1); for this reason, there is a formula for the number of integral octonions (elements of  $\Omega$ ) of any given norm:

$$\#\{\omega \in \Omega : N(\omega) = n\} = 240 \cdot \sum_{d|n} d^3.$$

There is a connection between Bhargava's cubes and Coxeter's integral octonions, arising from modular forms on exceptional groups. In my work on  $D_4$  modular forms, the following quantities arise: Suppose that  $C$  is a projective cube, in normal form, with  $\Delta = \Delta(C) < 0$ :



Let  $Emb(C, \Omega)$  denote the cardinality of the set:

$$\left\{ \begin{array}{l} (\alpha, \beta, \gamma) \in \Omega^3 \text{ such that} \\ N\alpha = -e, N\beta = -f, N\gamma = -g, Tr(\alpha\beta\gamma) = m \end{array} \right\}.$$

**Theorem 2 (M. W.)** *If  $C$  and  $C'$  are in the same  $SL_2(\mathbb{Z})^3$ -orbit, then  $Emb(C, \Omega) = Emb(C', \Omega)$ . The numbers  $Emb(C, \Omega)$  are the Fourier coefficients (indexed by cubes) of a “theta function” for the group  $Spin_{4,4}$ .*

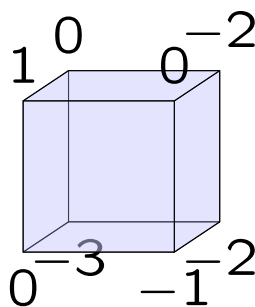
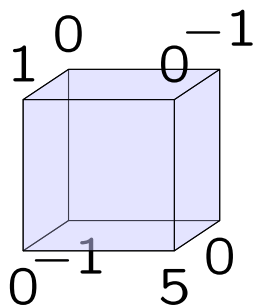
The quantities  $Emb(C, \Omega)$  should be machine-computable, especially for cubes of small (and perhaps prime) discriminant. These quantities should be identifiable with the Fourier coefficients of an Eisenstein series, but this has not yet been proven.

## Computations and questions

Bhargava's theorem, and the previous result, suggests that one should carry out the following:

- Choose a negative discriminant  $\Delta$ .
- Choose a triple  $[Q_1][Q_2][Q_3] = [1]$  of classes of binary quadratic forms of negative discriminant  $\Delta$ .
- Find a cube  $C$  which “encodes” these classes by slicing.
- Compute the quantity  $Emb([Q_1], [Q_2], [Q_3], \Omega) = Emb(C, \Omega)$ .

Below are two cubes of discriminant  $-20$  for experimentation.



The quantities  $Emb(C, \Omega)$  fit into a general class of embedding problems including the following:

- The classical “representation of quadratic forms by quadratic forms” problem can be rephrased as counting embeddings of a definite quadratic lattice into another definite quadratic lattice.
- If  $K$  is a quadratic imaginary field, and  $A$  is a maximal order in  $K$ , and  $\epsilon$  is the Dirichlet character associated to  $K/\mathbb{Q}$ , then  $Emb(A, \Omega)$  (the number of unital algebra embeddings) is equal to  $-252L(\epsilon, -2)$  by a result of Gross-Elkies\*.

In particular, I would hypothesize that  $Emb(C, \Omega)$  can be computed via an Euler product. The specific form of this product should be “guessable” from enough computations.

\*B. Gross and N. Elkies, [Embeddings into the integral octonions](#), Pac. J. of Math., 1997

Observe that  $Emb([Q_1], [Q_2], [Q_3], \Omega)$  assigns an integer to each “collinear” triple in a class group. There are some immediate questions:

Do these integers depend the elements in the class group? Do the integers only depend upon the genus of the quadratic forms, or the spinor genus?

Do these integers “look different” (bigger or smaller), when the structure of the class group is different (e.g., cyclic of order 4 or the Klein 4-group)? Can one see differences in the fine structure of the class group from these integers (a la Cohen-Lenstra)?

Can one guess a simple Euler product, or less simple but well-known L-value for the numbers  $Emb(C, \Omega)$ ? The degrees of the Euler factors should be guessable by computing dimensions of Lie algebras over finite fields.