OCTONIONS, CUBES, EMBEDDINGS

MARTIN H. WEISSMAN
MARCH 2, 2009

Octonions

Let k be a field, with $char(k) \neq 2$. A **Hurwitz algebra** over k is a finite-dimensional, unital, k-algebra A, together with a quadratic form $N\colon A \to k$, 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.

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 $\overline{(u, v)} = (\bar{u}, -v)$.

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 $f\colon \mathbf{P}^2(\mathbb{F}_2) \times \mathbf{P}^2(\mathbb{F}_2) \to \mathbb{F}_2$ 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 $\overline{e_{\vec{x}}} = -e_{\vec{x}}$.

Resulting structures on a Hurwitz algebra A include a trace,

$$Tr(a) = N(a+1) - N(a) - N(1),$$

and involution $\bar{a} = Tr(a) - a$. Hurwitz algebras are quadratic:

$$a^2 - Tr(a) + N(a) = 0.$$

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.

If $b \in B$, then $\bar{b} = Tr(b) - b$ denotes the main involution.

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

Nonsplit here means that the quadratic form is anisotropic

Elements of $\mathbf{P}^2(\mathbb{F}_2)$ are often called $e_1, e_2, e_3, e_4, e_5, e_6, e_7$ in the literature. This construction of an octonion algebra is due to Freudenthal.

Given a long history of mistakes is the subject, the signs given by $f(\vec{x}, \vec{y})$ should be machine-verified: one should verify that one gets an alternative algebra from this choice of signs, by considering quantities like $(e_{\vec{x}}e_{\vec{y}})e_{\vec{x}}$, which should equal $e_{\vec{x}}(e_{\vec{y}}e_{\vec{x}})$.

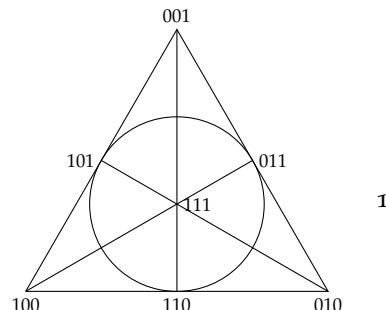Figure 1: The Fano plane. The label *abc* refers to the line through $(a, b, c) \in \mathbf{P}^2(\mathbb{F}_2)$.

Bhargava Cubes

The results on this page are all due to Manjul Bhargava[1] Define a **Bhargava cube** to be an element $C \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2$.

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:

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

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

Theorem 1 (Bhargava) *Fix an integer Δ. The orbits of $SL_2(\mathbb{Z})^3$ on the set of projective Bhargava cubes of discriminant Δ 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 Δ, 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:

$$Q_1(x, y) = x^2 + 5y^2.$$
$$Q_2(x, y) = 3x^2 - 2xy + 2y^2.$$

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

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

Since $[Q_3] = [Q_2]$ and $[Q_1] = [1]$, $[Q_2] \cdot [Q_2] = [1]$.
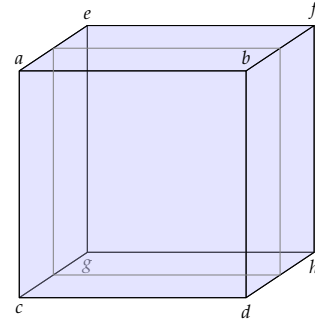
Figure 2: A Bhargava cube. Slicing along the light line yields the two matrices:

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

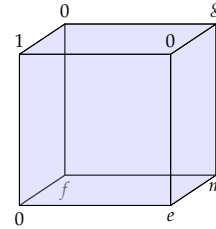$$N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Figure 3: A Bhargava cube in normal form. The three resulting quadratic forms, all of discriminant $\Delta = m^2 + 4efg$, are:

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

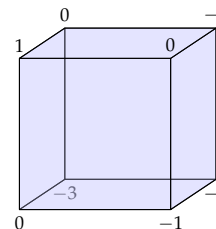$$Q_2(x, y) = -fx^2 + mxy + egy^2,$$

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

Figure 4: A Bhargava cube of discriminant -20.

Orders and an Embedding Question

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[2], after many mistaken attempts (e.g. by Kirmse). There exists a maximal order Ω, which contains Ω_{ng} with index 16; Coxeter describes this order explicitly.

The following statements characterize the order Ω as a lattice containing Ω_{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 Ω. Furthermore, Ω 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 Ω (unique up to conjugation by $Aut(\mathbb{O}/k)$) 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 Ω) of any given norm:

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

[2] H.S.M. Coxeter, **Integral Cayley Numbers**, Duke Math J., 1946

The history of mistakes, and the fact that our description of O differs from Coxeter's, suggests we should recompute the correct maximal order Ω, and check our work using computer assistance. First,

$$\Omega_{ng} \subset \Omega \subset 1/2\Omega_{ng}.$$

One should check that the lattice Ω has the following properties: the lattice, with the norm form, is isometric to the E_8 root lattice (with 240 elements of norm 1). It should also be closed under multiplication.

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[3], the following quantities arise: Suppose that C is a projective cube, in normal form, with $\Delta = \Delta(C) < 0$, as pictured on the right.

Define:

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

This counts the number of embeddings of "QT-structures" (triples of quadratic lattices endowed with a trilinear form), from a QT-structure coming from a Bhargava cube, into the QT-structure arising from $\mathbb{O}$ (with the norm quadratic form and the trace trilinear form).

Theorem 2 *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 seris, but this has not yet been proven.

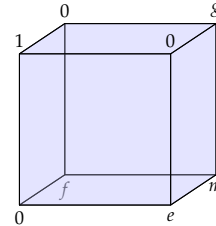[3] M. Weissman, D_4 **Modular Forms**, Amer. J. of Math., 2006

Figure 5: A Bhargava cube in normal form. Suppose that $\Delta = m^2 + 4efg < 0$.

For three octonions α, β, γ, it happens that

$$Tr((\alpha\beta)\gamma) = Tr(\alpha(\beta\gamma)).$$

Call this quantity $Tr(\alpha\beta\gamma)$.

Computations and questions

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

- Choose a negative discriminant Δ.

- Choose a triple $[Q_1][Q_2][Q_3] = [1]$ of classes of binary quadratic forms of negative discriminant Δ.

- Find a cube C which "encodes" these classes by slicing.

- Compute the quantity $Emb([Q_1], [Q_2], [Q_3], \Omega) = Emb(C, \Omega)$.

Such quantities 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 ϵ 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[4].

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.

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.

Any such answers could be helpful. Since these integers are the coefficients of a theta function on $Spin_{4,4}$, analytic techniques are available to estimate (bound) these integers as the discriminant grows.
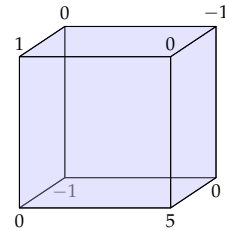

Figure 6: A Bhargava cube in normal form, with $\Delta = -20$. It reflects the identity $[1] \cdot [1] \cdot [1] = [1]$
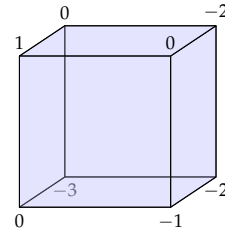

Figure 7: A Bhargava cube in normal form, with $\Delta = -20$. It reflects an identity $[Q] \cdot [Q] = [1]$

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

Suggested computational project, involving $Emb(C, \Omega)$ for the two cubes above: Count triples $(\alpha, \beta, \gamma) \in \mathbf{O}^3$ such that $N\alpha = 1$, $N\beta = 2$, $N\gamma = 3$, $Tr(\alpha\beta\gamma) = -2$. Then, count triples $(\alpha, \beta, \gamma) \in \mathbf{O}^3$ such that $N\alpha = 1$, $N\beta = 1$, $N\gamma = 5$, and $Tr(\alpha\beta\gamma) = 0$. One can definitely use tricks to speed up the brute force! Do these counts yield the same result? What are the results?

The fact that these integers are given by an Euler product is probably not difficult to prove. But, there might be some very bad Euler factors, arising from masses of nonmaximal lattices in a rank 3 Hermitian space.