Borcherds' proof of the moonshine conjecture

pjc, after V. Nikulin

Abstract

These CSG notes contain a condensed account of a talk by V. Nikulin in the London algebra Colloquium on 24 May 2001. None of the content is original to me: it is provided simply as a service for those who missed Nikulin's talks.

I have relied mainly on my notes from the lectures, So any errors are the product of the note-taking and are not to be attributed to the content of the lectures.

1 The monster

The monster, or Fischer-Griess group, $\mathbb{M}$ (otherwise known as the Friendly Giant) is the largest sporadic simple group. Its order is

$$\begin{aligned}&808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000\\&= 2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71.\end{aligned}$$

It was discovered by Fischer and Griess in 1973 and constructed by Griess in 1982.

The Monster has 194 conjugacy classes (a very small number for a simple group of this size). The smallest faithful permutation representation has degree roughly 10^{30} (very large). The smallest faithful matrix representation over $\mathbb{C}$ has degree 196 883; the second smallest, 21 296 876.

Griess constructed $\mathbb{M}$ as the automorphism of a commutative non-associative algebra with identity on a real vector space of dimension 196 884 (on which it acts as the sum of the trivial representation and the representation of degree 196 883). This algebra also has an $\mathbb{M}$-invariant inner product, since the representation of $\mathbb{M}$ is self-dual. This algebra is known as the *Griess algebra*.

2 Modular functions

The *modular group* $\mathrm{PSL}(2,\mathbb{Z})$ is the group of linear fractional transformations

$$\tau \mapsto \frac{a\tau+b}{c\tau+d},$$

for $a,b,c,d \in \mathbb{Z}$, $ad-bc=1$. It can be regarded as a group of transformations of the upper half-plane $\mathbb{H}$ (including the point ∞).

A *modular function* f is a complex function on the upper half plane which is *meromorphic* (i.e. analytic except for a discrete set of poles) and satisfies

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau)$$

for all transformations in $\mathrm{PSL}(2,\mathbb{Z})$.

Since the modular group contains in particular the transformation $\tau \mapsto \tau+1$, we see in particular that modular function is periodic with period 1. By the theory of Fourier series, it can be written in terms of the variable $q = \mathrm{e}^{2\pi \mathrm{i} \tau}$. (More specifically, the Laurent series for f in terms of q is the Fourier series for f in terms of τ.) By abuse of notation we will sometimes write $f(q)$ instead of $f(\tau)$.

It can be shown that the modular functions form a field isomorphic to the field of rational functions in one variable over $\mathbb{C}$. A generator for this field is called a *main modular function*, or *Hauptmodul*. As function of q, it has a pole of order 1 at the origin, and is said to be *normalised* if its Laurent series begins

$$f(q) = q^{-1} + 0 \cdot q^0 + \cdots.$$

There is a unique normalised main modular function, usually denoted by j. It has the remarkable expression

$$j + 744 = \frac{\left(1 + 240 \sum_{n \geq 0} \sigma_3(n) q^n\right)^3}{q \prod_{n>0} (1-q^n)^{24}},$$

where

$$\sigma_3(n) = \sum_{d|n} d^3.$$

Its Fourier series begins

$$j(q) = q^{-1} + 196\,884q + 21\,493\,760q^2 + \cdots.$$

More generally, if H is any subgroup of the modular group, a modular function for H is a meromorphic function on the upper half-plane which is invariant under the transformations in H. If H has *genus zero* (this means that the quotient of $\mathbb{H}$ by H is isomorphic to the Riemann sphere), then the field of H-modular functions again form a field isomorphic to the rational functions in one variable, and we can define a normalised main modular function for H as before. It turns out that there are about 370 subgroups of genus zero in the modular group; all satisfy

$$\Gamma_0(N) \leq H \leq \Gamma_0(N)^+$$

for some N, where $\Gamma_0(N)$ consists of all the modular transformations with $c \equiv 0 \pmod{N}$, and $\Gamma_0(N)^+$ is its normaliser in $\mathrm{PSL}(2,\mathbb{Z})$.

3 Moonshine

John McKay pointed out the remarkable similarity of the numbers 196 883 (the smallest non-trivial character degree of $\mathbb{M}$) and 196 884 (the coefficient of q in the modular function j). Looked at another way, the number 196 884 occurs in both contexts, as the dimension of the Griess algebra for $\mathbb{M}$ and the coefficient of the modular function.

Moreover, the coefficient of q^2 in $j(q)$ is

$$21\,493\,760 = 1 + 196\,883 + 21\,296\,876,$$

the sum of the three smallest character degrees.

These observations led to the first part of the *moonshine conjecture* of Conway and Norton:

Conjecture 1: There is a graded $\mathbb{M}$-module

$$V = \bigoplus_{m \geq -1} V_m$$

with $\dim(V_m) = c(m)$ for all $m \geq -1$, where

$$j(q) = \sum_{m \geq -1} c(m) q^m.$$

But there were even more surprises in store. If this conjecture is true, then for each element $g \in \mathbb{M}$, the element g acts on V_m, and has a character value

$$\chi_m(g) = \text{Trace}(g \mid V_m).$$

Then we can form the so-called *Thompson series* of g,

$$T_g(q) = \sum_{m \geq -1} \chi_m(g) q^m.$$

Note that since V_{-1} affords the trivial character and V_0 is the zero space, we have

$$T_g(q) = q^{-1} + 0 \cdot q^0 + \cdots.$$

The second part of the moonshine conjecture states:

> **Conjecture 2:** With V as in Conjecture 1, for every element $g \in \mathbb{M}$, there is a genus-zero subgroup H of the modular group such that $T_g(q)$ is the normalised main modular function for H.

Note that $T_g(q) = T_{g^{-1}}(q) = T_{g^x}(q)$ for all $g, x \in \mathbb{M}$, so that instead of one assertion (and one genus-zero subgroup) for each element of the monster, we only have one for each inverse pair of conjugacy classes. There are 171 inverse pairs of conjugacy classes. So fewer than half of the genus-zero subgroups arise in this connection. It is not understood what distinguishes the ones which do appear from the others.

4 Outline of Borcherds' proof

Borcherds' proof, "Monstrous moonshine and monstrous Lie superalgebras", *Invent. Math.* **102** (1992), 405–444, proceeds in five steps:

4.1. Construct a *vertex operator algebra* V, a graded algebra affording the moonshine representations of $\mathbb{M}$.

4.2. Construct a Lie algebra M from V; this M is a *generalised Kac–Moody Lie algebra*.

4.3. Construct a *denominator identity* for M related to the coefficients of $j(q)$.

4.4. Construct *twisted denominator identities* similarly related to the series $T_g(q)$.

4.5. Complete the proof.

Note that, although the module V is constructed in the first step, the properties needed to prove the moonshine conjecture are not established until the end of the proof.

4.1 The vertex operator algebra

Vertex operator algebras arise in physics and are connected with conformal field theory. It was Borcherds who first wrote down axioms for them.

A vertex operator algebra consists of a real vector space V with a unit or "vacuum" 1, a conformal vector or "central charge" w with a "dimension" $c \in \mathbb{R}$, and a binary operation denoted $u_m v$ for $m \in \mathbb{Z}$ satisfying various axioms. Among these are the fact that V is graded, with $1 \in V_0$ and $c \in V_2$; a version of the Jacobi identity; a "conformal vector" axiom stating

$$[L_m, L_n] = (m-n)L_{m+n} + \binom{m+1}{3}\frac{c}{2}\delta_{m,-n}$$

where $L_m(v) = w_{m+1} v$ (so that $\langle L_m : m \in \mathbb{Z}\rangle$ is a representation of the *Virasoro algebra*), and a "conformal weight" axiom asserting that $L_0(v) = w_1 v = \mathrm{wt}(v)v$ (so that the grading is by eigenspaces of L_0).

How do vertex operators get into the act? They are defined by

$$Y(u,z) = \sum_m u_m (.) z^{-m-1} \in \mathrm{End}(V)[[z, z^{-1}]].$$

They can be used to simplify the axioms, e.g. we have

- $Y(1,z) = 1$,
- $\dfrac{\mathrm{d}}{\mathrm{d}z} Y(u,z) = Y(L_{-1}u, z)$.

It follows from the axioms that, for $u, v \in V_2$,

- $u * v = u_1 v \in V_2$ defines a commutative, non-associative algebra on V_2;
- $\langle u, v\rangle \cdot 1 = u_3 v \in V_0$ defines an inner product on V_2.

Now, roughly speaking, the moonshine module V for $\mathbb{M}$ is the vertex operator algebra "generated" by the 196 884-dimensional Griess algebra, with the multiplication and inner product identified with those given above. However, a great deal of ingenuity is required; it is not simply a case of applying an obvious functor! There is one more, very small, complication: we have to shift the dimensions down by 1, since the construction gives $\dim(V_0) = 1$, $\dim(V_1) = 0$.

Borcherds simply mentioned the existence of the module in a short paper "Vertex algebras, Kac–Moody algebras, and the Monster", *Proc. National Academy USA* **83** (1986), 3068–3071. The details are spelt out in the 520-page book *Vertex operator algebras and the Monster* by Frenkel, Lepowski and Meurman, Academic Press 1988.

4.2 The monster Lie algebra

The Lie algebra M is graded by the lattice $\mathrm{II}_{1,1}$ consisting of the set $\mathbb{Z}^2$ with quadratic form given by $(m,n)^2 = -2mn$. That is, M has components $M_{(m,n)}$ for $m,n \in \mathbb{Z}$ satisfying $\dim(M_{(m,n)}) < \infty$ for all m,n. It satisfies

- $M_{(0,0)} \cong \mathrm{II}_{1,1} \otimes \mathbb{R} = \mathbb{R}^2$,
- for $(m,n) \neq (0,0)$, $M_{(m,n)} \cong V_{mn}$ as $\mathbb{M}$-module, so that $\dim(M_{(m,n)}) = c(mn)$.

(Since we haven't yet proved Conjecture 1, $c(m)$ here means $\dim(V_m)$; it will turn out to be equal to the coefficient of q^m in $j(q)$.)

Hence the non-zero components of M are

- $M_{(0,0)}$, with dimension 2;
- $M_{(1,-1)}$ and $M_{(-1,1)}$, each with dimension 1;
- $M_{(m,n)}$ for all integer points (m,n) strictly in the first or third quadrant, with $M_{(m,n)} \cong V_{mn}$.

The corresponding vectors $(m,n) \neq (0,0)$ are the *roots* of the Lie algebra. Let Δ be the set of roots. We call a root *real* or *imaginary* according as its square is positive or negative (using the quadratic form $(m,n)^2 = -2mn$). Thus, there are two real roots and infinitely many imaginary ones. The *positive roots* are those with $m > 0$.

The *Weyl group* W is generated by reflection in the line perpendicular to the real roots; it is cyclic of order 2 generated by $(m,n) \mapsto (n,m)$. The *Weyl vector* is $\rho = (-1,0)$; it satisfies $(\rho,\alpha) = -\alpha^2/2$ for any simple real root α.

The monster Lie algebra M is a *generalised Kac–Moody Lie algebra*. That is to say, it is generated by elements h_α, e_α, f_α for simple roots α, satisfying:

- the h_α commute and generate the *Cartan subalgebra* $M_{(0,0)}$;
- $[h_\alpha, e_{\alpha'}] = (\alpha, \alpha')e_{\alpha'}$;
- $[h_\alpha, f_{\alpha'}] = -(\alpha, \alpha')f_{\alpha'}$;
- $[e_\alpha, f_{\alpha'}] = \delta_{\alpha\alpha'}h_\alpha$;
- $\mathrm{ad}(e_\alpha)^{1-2(\alpha,\alpha')\alpha^2}e_{\alpha'} = 0$ if $\alpha^2 > 0$, and similarly with f in place of e.

4.3 The denominator identity

Any generalised Kac–Moody Lie algebra has a *denominator identity*. This is an identity in the integral semigroup ring of the root lattice (spanned by elements e^α for all roots α) given by

$$e^\rho \prod_{\alpha\in\Delta_+} (1-e^\alpha)^{\mathrm{mult}(\alpha)} = \sum_{w\in W} (\det w) w\left(e^\rho \sum_r \varepsilon(r) e^r\right),$$

where $\mathrm{mult}(\alpha)$ is the dimension of the component indexed by α, and r is a sum of pairwise orthogonal simple imaginary roots.

In our case, write $e^{(m,n)} = p^m q^n$, where $p = e^{(1,0)}$ and $q = e^{(0,1)}$. Thus, the left-hand side is simply

$$p^{-1} \prod_{m>0,\, n} (1-p^m q^n)^{c(mn)}.$$

Note that this can be rewritten as

$$p^{-1} \sum_{m,k>0,\, n} c(mn) p^{mk} q^{nk}/k.$$

For the right-hand side, we have a simplification since no two imaginary simple roots are orthogonal (they lie strictly in the first quadrant), and so it reduces just to $j(p) - j(q)$, where $j(p) = \sum_m c(m)p^m$. So we have the identity

$$p^{-1} \prod_{m>0,\, n} (1-p^m q^n)^{c(mn)} = j(p) - j(q).$$

Note that the usual situation in a GKM Lie algebra is that we know the right-hand side and use the denominator identity to calculate the multiplicities of the roots; here the procedure is reversed.

4.4 Twisted versions

Taking the trace of an arbitrary element of $\mathbb{M}$, we come to the *twisted denominator identities*:

$$p^{-1}\exp\left(-\sum_{m,k>0,\,n} c_{g^k}(mn)p^{mk}q^{nk}/k\right) = \sum_m c_g(m)p^m - \sum_n c_g(n)q^n = T_g(p) - T_g(q),$$

where $c_g(m)$ is the trace of g on V_m.

They are in fact denominator identities of suitable GKM Lie superalgebras.

4.5 Completion of the proof

The denominator identity can be shown to determine the numbers $c(m)$. Indeed, it can be shown that $c(1)$, $c(2)$, $c(3)$ and $c(5)$ determine all the other values. It can be checked directly by computation that these four numbers agree with the corresponding coefficients in the modular function. So in order to make the identification, we have to show that the coefficients of $j(q)$ are determined by the same rule.

There are two techniques for doing this, both quite complicated. One uses *Hecke operators*, the other uses *Lie algebra homology* and *Adams operators*. I will not even attempt to sketch these!

Similarly the numbers $c_g(m)$ occurring as coefficients in the Thompson series are determined by the values for $m = 1,2,3,5$, which can be read off from the character table of $\mathbb{M}$; indeed we have

$$\begin{aligned}
\chi(V_1) &= \chi_1 + \chi_2,\\
\chi(V_2) &= \chi_1 + \chi_2 + \chi_3,\\
\chi(V_3) &= 2\chi_1 + 2\chi_2 + \chi_3 + \chi_4,\\
\chi(V_5) &= 4\chi_1 + 5\chi_2 + 3\chi_3 + 2\chi_4 + \chi_5 + \chi_6 + \chi_7,
\end{aligned}$$

where $\chi_1,\ldots,\chi_7$ are the seven smallest characters of $\mathbb{M}$.

So, once the appropriate genus-zero subgroups of the modular group have been identified, just 171×4 numerical verifications complete the proof.