Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 347–353

The Essentials of Monstrous Moonshine

John McKay

This is a fast introduction to Monstrous Moonshine.

All our functions expanded at $\tau = i\infty$ have the form:

$$(*) \qquad f(\tau) = \frac{1}{q} + \sum_{k \geq 0} a_k q^k, \quad q = e^{2i\pi\tau}, \quad \Im(\tau) > 0, \quad a_k \in \mathbb{C}.$$

We further assume that $a_0 = 0$ (standard form) for convenience, and that $a_k \in \mathbb{Q}$ (to ensure trivial Galois action). For replicable functions there is a reasonable conjecture that the a_k are algebraic integers - this, too, we assume. We find that the coefficients of classical modular functions known to Jacobi, Fricke, and Klein, are related to the characters of $\mathbb{M}$, the Monster simple sporadic group, in that, to each conjugacy class of cyclic subgroups $\langle g \rangle$, of $\mathbb{M}$, there is such a function, j_g with coefficient of $q^k = \mathrm{Trace}\big(H_k(g)\big)$ for some representation, H_k, (the k^{th} Head representation) of $\mathbb{M}$.

In November 1978 I wrote to John Thompson that $196884 = 1 + 196883$, relating the coefficient of q in the elliptic modular function, $j(\tau)$, to the degree of the smallest faithful complex representation of $\mathbb{M}$. Little was then known to me of the degrees of irreducible characters of $\mathbb{M}$ but I did have access to those of $E_8(\mathbb{C})$ and related an initial sequence of them to the q-coefficients of the cube root of j. This was quickly disposed of by Victor Kac [Kac], see also [Lep].

There are 194 conjugacy classes of $\mathbb{M}$, 172 classes of cyclic subgroups, and 171 distinct functions j_g. This, and more, is to be found in Conway-Norton [CN]. All these functions are genus zero in that this is the genus of the compactified Riemann surface $\widehat{G_f \backslash \mathcal{H}}$ where G_f is the discrete invariance group of f, acting on the upper half-plane, $\mathcal{H}$.

Research supported by the Natural Sciences and Engineering Research Council (Canada), and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Québec)

Received August 25, 2000.

By axiomatizing the properties of these functions, we arrive at the notion of a replicable function, as one which behaves well under a generalized Hecke operator. These are now under scrutiny. My hope is that their properties will yield an intrinsic description of $\mathbb{M}$.

We study replicable functions, which generalize a degenerate family called by me the "modular fictions", namely $f(\tau) = 1/q + cq$. Cummins [CuN] has proved these are the unique replicable finite Laurent series, $(\forall k \geq k_0,\ a_k = 0)$. A further useful property to impose is that the replication power map (defined later): $f \to f^{(n)}$, is periodic, namely $\forall n \geq 1,\ f^{(\gcd(n,k))} = f^{(n)}$. When this is so, the modular fictions reduce to three cases, $1/q$, $1/q + q$, $1/q - q$, corresponding to exp, cos, and sin respectively. An amusing consequence of their replicability is that $\sin(2kt)$ is not a polynomial in $\sin(t)$, whereas $\cos(2kt)$ is a polynomial in $\cos(t)$. This follows from a study of the modular equation [Sil], [Mar] for f, with formal coefficients [McK]. The modular fictions play no further part in what follows.

Replicable functions are generalizations of the prototype, $j(\tau)$, the elliptic modular function which is characterized by its form and the property under the action of Hecke operators [Serre]:

$$\forall n \geq 1,\ nT_n\big(j(\tau)\big) = \sum_{\substack{ad=n\\ 0\leq b<d}} j\Big(\frac{a\tau + b}{d}\Big) = P_{n,j}\big(j(\tau)\big),$$

where T_n denotes the standard Hecke operator, and $P_{n,j} = P_n$ is the Faber [Fab], [Cur] polynomial of degree n. The notation is to remind one that the coefficients of the Faber polynomial come from its argument.

One characterization of these polynomials is that

$$P_{n,f}(f) - \frac{1}{q^n} \in q\,\mathbb{C}[[q]].$$

We find

$$\begin{aligned}
P_{1,f}(f) &= f,\\
P_{2,f}(f) &= f^2 - 2a_1,\\
P_{3,f}(f) &= f^3 - 3a_1 f - 3a_2,\\
P_{4,f}(f) &= f^4 - 4a_1 f^2 - 4a_2 f + 2a_1^2 - 4a_3.
\end{aligned}$$

More generally:

$$P_{n,f}(f) = \det(fI - A_n)$$

where

$$A_n = \begin{pmatrix} a_0 & 1 & & & & \\ 2a_1 & a_0 & 1 & & 0 & \\ \vdots & \vdots & \vdots & & & \\ (n-2)a_{n-3} & a_{n-4} & a_{n-5} & \cdots & 1 & \\ (n-1)a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_0 & 1 \\ na_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \end{pmatrix}.$$

This is related to expressing the power sums in terms of elementary symmetric functions. Truncating f and replacing q by $1/x$, we derive: $F(x) = x^m + a_0x^{m-1} + \cdots + a_{m-1}$, $m \geq n$, and we may identify the $\{e_k\}$ with the elementary symmetric functions of the roots of $F(x)$. Note that the power sum $s_n \in \mathbb{Z}[a_0, \ldots, a_{n-1}]$.

Expanding $P_{n,f}\big(f(\tau)\big)$ in powers of q, the Grunsky [G] coefficients, $h_{m,n}$, are defined by

$$P_{n,f}\big(f(\tau)\big) = \frac{1}{q^n} + n \sum_{m \geq 1} h_{m,n}q^m.$$

We generalize j to a family of replicable functions (of standard form), $f^{(k)}$, $k \geq 1$, for which

$$\sum_{\substack{ad=n \\ 0 \leq b < d}} f^{(a)}\Big(\frac{a\tau + b}{d}\Big) = P_{n,f}\big(f(\tau)\big).$$

This yields a new Hecke operator, $\hat{T}_n$ with $h_{m,n}$ as the coefficient of q^m in $\hat{T}_n(f)$. It is Grunsky's law of symmetry that $h_{m,n} = h_{n,m}$.

We now have an inductive definition of the important "replication power map" taking f to $f^{(n)}$, since $f^{(n)}(n\tau) = P_{n,f}(f) - \sum'$ where $\sum'$ omits the single term with $a = n$. This imposes the condition that the right side is a series in q^n. We take the principal branch to define $f^{(n)}(\tau)$. The replication power map f to $f^{(n)}$, f replicable, restricts on Monstrous Moonshine functions to the map induced on them by taking $g \in \mathbb{M}$ to g^n. Norton [N], in an important paper, defines the generating functions for the Faber polynomials and the $h_{m,n}$, unaware of the work of Faber [Fab] and Grunsky [G] preceding him. He gives a definition of replicability equivalent to the above, [ACMS], namely (paraphrased):

Definition. A function is replicable if $\gcd(m,n) = \gcd(r,s)$ and $\operatorname{lcm}(m,n) = \operatorname{lcm}(r,s)$ implies $h_{m,n} = h_{r,s}$.

[This suggests seeking an interpretation of the $\{h_{m,n}\}$ in terms of double coset representatives.]

Norton also proves his basis theorem:

Theorem. *The twelve coefficients a_k,*

$$k \in \{1, 2, 3, 4, 5, 7, 8, 9, 11, 17, 19, 23\},$$

determine a replicable function.

This remarkable result is useful for computing with replicable functions.

Newton's relations, which derive from the form of f, between the a_k and the Faber polynomials, together with Norton's defining properties of the $\{h_{m,n}\}$, show that replicable functions correspond to K-points on a variety. Norton has proved that K lies in a composite of quadratic extensions of $\mathbb{Q}$.

The Newton relations are equivalent to the generating function identity:

$$q\big(f(q) - f(p)\big) = \exp(-\sum_{n\geq 1} P_{n,f}\big(f(p)\big)q^n),$$

with $p = \exp(2\pi i\sigma)$ etc., where we abuse notation using $f(p)$ and $f(q)$ instead of $f(\sigma), f(\tau)$.

There is an outstanding conjecture of Norton [CuG], [CuN]:

Conjecture 1.2. *A function $f = q^{-1} + \sum_{i\geq 1} a_i q^i$ with rational integer coefficients is replicable if and only if either f is a modular fiction or it is the Hauptmodul for a group $G \subset PGL_2(\mathbb{Q})^{>0}$ satisfying*

1. *G has genus zero,*
2. *G contains a finite index $\Gamma_0(N)$,*
3. *G contains $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$.*

Our model is Dedekind's (1877) [Ded] construction of $j(\tau)$ in terms of its Schwarz differential equation.

We define the Schwarz derivative $\{f, \tau\}$ to be $2(f''/f')' - (f''/f')^2$, where differentiation is with respect to τ. When f is a modular form, $\{f, \tau\}$ increases the weight by 4 and preserves the invariance properties, thus when f is a Hauptmodul, we have $\{f, \tau\} + R(f)f'^2 = 0$ with $R(f) = N(f)/[D(f)]^2$, the differential resolvent, and $f' = df/d\tau$ of weight 2. When expressed in partial fractions, we see $R(f)$ gives ramification data and also the critical points of f (namely those values of f for which $f'(\tau) = 0$).

From Dedekind (with normalization

$$1728\, j(\tau) = 1/q + 744 + 196884\, q + \cdots)$$

we find $R(j) = \frac{1-\frac{1}{2^2}}{(j-1)^2} + \frac{1-\frac{1}{3^2}}{j^2} - \frac{1-\frac{1}{2^2}-\frac{1}{3^2}}{j(j-1)}$, with ramification multiplicity 2 at $j\big(\exp(\pi i/2)\big) = 1$, and 3 at $j\big(\exp(\pi i/3)\big) = 0$.

To each f, there is a corresponding conformal invariance group, G_f acting on $\mathcal{H}$. From $R(f)$ we can find the critical points in $\mathcal{H}$, and the ramification gives the angles between bounding circular arcs intersecting at a critical point. A fundamental domain can be constructed and, once edges are identified, a presentation found for the group generated by hyperbolic reflections in the bounding circular arcs in $\mathcal{H}$. The Schwarz derivative takes us from f to G_f.

Over 600 Hauptmoduls, f, as above, are now known, some of which appear in [FMN]. For each, $R(f)$ has been computed. The Galois group of D is of "dihedral type", in that it has a unique cyclic subgroup of index 2. This provides an ordering of the critical points for Ohyama's construction of dynamical systems [Ohy1]. With a little more work, we should obtain a dynamical system of differential equations for each f, as shown by Ohyama [Ohy1] and exemplified by the Halphen system. This system was first studied in 1881 [Hal], and is a reduction of the self-dual Yang-Mills equations. For us, it is derived from the $\Gamma(4)$-Hauptmodul, namely $f = \big(\eta(\tau)/\eta(4\tau)\big)^8$. This has a triangular fundamental domain with angles $(0,0,0)$ at cusps $(0,1,\infty)$. It is remarkable that we have $\{f,\tau\} + E_4(2\tau) = 0$, where $E_4(\tau)$ is the Eisenstein series of weight 4:

$$E_4(\tau) = 1 + 240 \sum_{n\geq 1} \sigma_3(n) q^n.$$

In a further paper [Ohy2] the function $f = \big(\eta(\tau)/\eta(9\tau)\big)^3$ appears and we find it satisfies the Schwarz equation above with $E_4(2\tau)$ replaced by $E_4(3\tau)$.

Any function of the form $(*)$ satisfies

$$\frac{df}{dq} + \frac{1}{q^2}\exp(-v^t H v) = 0,$$

where $v^t = (q, q^2, q^3, \dots)$, and H is the semi-infinite matrix of Grunsky coefficients.

To each Hauptmodul there are two differential objects:

(1) A Schwarz equation, and
(2) a dynamical system.

There is also a pseudo-differential operator (roughly–treating the functions as Laplace transforms) which has not yet been studied.

A purpose of this approach is to learn more about analytic aspects associated with the Monster in the hope of better understanding the relation between the simple Lie groups and the sporadic simple groups.

Witten's ideas suggest there may be a finite-dimensional spin manifold with $\mathbb{M}$ acting on its loop space. A discussion of this is found in the book [Hir].

References

[ACMS] Alexander, D., Cummins, C., McKay, J., and Simons, C., Completely replicable functions, Lond. Math. Soc. Lecture Notes, **165**, edited by Liebeck and Saxl (1992), 87–98.

[CN] Conway, J.H., and Norton, S.P., Monstrous moonshine, Bull. Lond. Math. Soc., **11** (1979), 308–339.

[CuG] Cummins, C. J. and Gannon, T., Modular equations and the genus zero property of Moonshine functions, Inv. Math., **129** (1997), 413–443.

[CuN] Cummins, C. J. and Norton, S.P., Rational Hauptmoduls are replicable, Can. J. Math., **47** (1995), 1201–1218.

[Cur] Curtiss, J. and H., Faber polynomials and the Faber series, Amer. Math. Monthly **78** and **79** (1974), 577–596 and 363.

[Ded] Dedekind, R., Schreiben an Herrn Borchardt über die Theorie der elliptischen Modulfunktionen, Crelle, **83**, 265–292.

[Fab] Faber, G., Über polynomische Entwicklungen, Math. Annalen, **57** (1903), 389–408.

[FMN] Ford, D.J., McKay, J., and Norton, S.P., More on replicable functions, Comm. in Alg., **22** (1994), 5175–5193.

[G] Grunsky, H., Koeffizientenbedingungen für schlicht abbildende meromorphe Funktionen, Math. Z., **45** (1939), 29–61.

[Hir] Hirzebruch, F., Berger, T. and Jung R., "Manifolds and Modular Forms (Vieweg)", 1992.

[Kac,] Kac, V., An elucidation of: "Infinite-dimensional algebras, Dedekind's η-function, classical Möbius function and the very strange formula". $E_8^{(1)}$ and the cube root of the modular invariant j, Adv. in Math., **35** (1980), 264–273.

[Lep] Lepowsky, J., Euclidean Lie algebras and the modular function j, "Proc. Symp. Pure Math., **37**, Amer. Math. Soc.", 1980, pp. 567–570.

[Mar] Martin, Y., On modular invariance of completely replicable functions, Contemp. Math., **193** (1996), 263–286.

[McK] McKay, J., The formal modular equation, (unpublished).

[N] Norton, S.P., More on moonshine, "Computational group theory, edited by M.D. Atkinson, Academic", 1984, pp. 185–193.

[Ohy1] Ohyama, Y., Systems of nonlinear differential equations related to second order linear equations, Osaka J. Math., **33** (1996), 927–949.

[Ohy2] Ohyama, Y., Differential equations for modular forms with level three, To appear (),.

[Ser] Serre, J-P., "A course in arithmetic, Springer-Verlag", 1973.

[Sil] Silverman, J.H., "Advanced topics in the arithmetic of elliptic curves, Springer-Verlag", 1994, pp. 181.

Centre Interuniversitaire en
Calcul Mathématique Algébrique
Concordia University
Montreal
Canada
email: mckay@cs.concordia.ca