ANNALES DE L'I. H. P., SECTION A

TERRY GANNON

The classification of $SU(3)$ modular invariants revisited

Annales de l'I. H. P., section A, tome 65, nº 1 (1996), p. 15-55
<http://www.numdam.org/item?id=AIHPA_1996__65_1_15_0>

Ann. Inst. Henri Poincaré,

Vol. 65, n° 1, 1996, p. 15-55. *Physique théorique*

The classification of SU(3) modular invariants revisited

by

Terry GANNON

Department of Math, Concordia University,
1455 de Maisonneuve Blvd,
Montréal, Canada H3G 1M8.

Dedicated to the memory of Claude Itzykson

ABSTRACT. – The SU(3) modular invariant partition functions were first classified in ref. [1]. Here we accomplish the SU(3) classification using only the most basic facts: modular invariance; $M_{\lambda\mu} \in \mathbf{Z}_{\geq}$ and $M_{00} = 1$ (in [1], the Moore-Seiberg naturality "theorem" for partition functions was also used). A number of significant simplifications to the general argument are included here. Hidden in [1] were a number of smaller results which could be of independent value. These are explicity mentioned here. We also include a survey of known tools for WZW classifications, and sketch the beginnings of a program for classifying all WZW partition functions for any affine algebra g – indeed the proof here has been designed specifically to suggest this generalization.

RÉSUMÉ. – Les fonctions de partition invariantes modulaires pour SU(3) étaient classifiées dans la référence [1]. Dans ce mémoire, nous établissons la classification de SU(3) utilisant seulement les faits les plus fondamentaux : l'invariance modulaire; $M_{\lambda\mu} \in \mathbf{Z}_{\geq}$; et $M_{00} = 1$ (quelques résultats moins élémentaires obtenus par Moore et Seiberg étaient utilisés par la référence [1]). Nous incluons dans ce mémoire plusieurs simplifications à la preuve, ainsi que certains résultats additionnels de moindre importance. Le thème majeur est celui de la généralisation à une algèbre arbitraire g.

1. INTRODUCTION

This paper focuses on the classification of A_2 Wess-Zumino-Witten partition functions. This was first accomplished in ref. [1]. There are two main purposes of this paper: to do the classification assuming only (P1), (P2), and (P3) (defined later this section)[1] – in ref. [1] some less elementary results from [2] were required; and to rewrite the proof so that a possible generalization to all other algebras begins to take shape. In the process, we get a proof which is both more explicit and in most places far simpler. Most of the underlying statements and formulae will be made for A_2, but can be naturally extended to any algebra. It should be stressed however that in spite of the significant recent progress ([25], [26], [29]) which this paper incorporates, much remains to be done before the classification for general g can be realized. (This point is discussed in more detail in the conclusion.)

A *partition function* for A_2 WZW theories at level k (we write this $A_{2,k}$) looks like

$$Z(\tau, z) = \sum_{\lambda, \mu \in \mathcal{P}^k} M_{\lambda\mu} \chi_\lambda^k(\tau, z, 0) \chi_\mu^k(\tau, z, 0)^*. \tag{1.1}$$

χ_λ^k is the *normalized character* [3] of the representation of the affine Kac-Moody algebra $A_2^{(1)}$ with (horizontal, ρ-shifted) highest weight λ and level k; it can be throught of as a complex-valued function of the Cartan subalgebra of $A_2^{(1)}$, *i.e.* a function of a complex 2-vector z and complex numbers τ, u (we will always take $u = 0$). The (finite) sum in equation (1.1) is over the horizontal ρ-shifted highest weights λ, $\mu \in \mathcal{P}^k$ of level k:

$$\mathcal{P}^k = P_{++}^{k+3} \stackrel{\text{def}}{=} \{ (\lambda_1, \lambda_2) | \lambda_1, \lambda_2 \in \mathbf{Z}, 0 < \lambda_1, \lambda_2, \lambda_1 + \lambda_2 < k+3 \}. \tag{1.2}$$

We will always identify a weight λ with its Dynkin labels λ_1, λ_2 – e.g. $\rho = (1, 1)$. The quantity $k + 3$ will appear throughout. It is called the *height* and will be denoted n.

The characters χ in this paper will depend on a complex 2-vector z. Many people working on these problems use "restricted characters", *i.e.* put $z = 0$. However, this seems to be a mistake, and the math (if not the physics) appears to demand that z be included.

Because (and only because) we have $z \neq 0$, there is a one-to-one correspondence between the partition function Z and its coefficient matrix M. We will freely identify them.

---

[1] The desirability of doing this was most emphatically made to the author by Claude Itzykson.

The characters χ_λ^k for fixed k define a unitary representation [4] of the modular group $SL(2, \mathbf{Z})$. In particular:

$$\chi_\lambda^k(\tau+1, z) = \sum_{\mu\in\mathcal{P}^k} (T^{(n)})_{\lambda\mu}\,\chi_\mu^k(\tau, z), \tag{1.3a}$$

$$(T^{(n)})_{\lambda\mu} \stackrel{\text{def}}{=} \exp\left[2\pi i\,\frac{\lambda_1^2+\lambda_1\lambda_2+\lambda_2^2-n}{3n}\right]\delta_{\lambda\mu}; \tag{1.3b}$$

$$\exp[-k\pi i z^2/\tau]\,\chi_\lambda^k(-1/\tau, z/\tau) = \sum_{\mu\in\mathcal{P}^k} (S^{(n)})_{\lambda\mu}\,\chi_\mu^k(\tau, z), \tag{1.3c}$$

$$(S^{(n)})_{\lambda\mu} \stackrel{\text{def}}{=} \frac{-i}{n\sqrt{3}}\sum_{w\in W} \det w\,\exp\left[-2\pi i\,\frac{w(\lambda)\cdot\mu}{n}\right]. \tag{1.3d}$$

W in (1.3*d*) is the A_2 Weyl group. The matrices $T^{(n)}$ and $S^{(n)}$ are unitary and symmetric.

Our task will be to find all Z in equation (1.1) satisfying the following 3 properties:

(P1) *modular invariance*. This equivalent to the matrix equations:

$$T^{(n)\dagger}MT^{(n)} = M, \qquad i.e.\quad MT^{(n)} = T^{(n)}M, \tag{1.4a}$$

$$S^{(n)\dagger}MS^{(n)} = M, \qquad i.e.\quad MS^{(n)} = S^{(n)}M; \tag{1.4b}$$

(P2) the coefficients $M_{\lambda\mu}$ in equation (1.1) must be non-negative integers; and

(P3) we must have $M_{\rho\rho} = 1$, where $\rho = (1, 1)$.

We will can any modular invariant function Z of the form equation (1.1), an *invariant*. Z will be called *positive* if in addition each $M_{\lambda\mu} \geq 0$, and *physical* if it satisfies (P1), (P2), and (P3). Our task is to find all physical invariants for each level k. There are other properties a physically reasonable partition function should satisfy, but for a number of reasons it is preferable to limit attention to as small a number of properties as possible. *In this paper, only (P1)-(P3) will be used.*

The A_2 classification problem has had a fairly long history. Ref. [5] tried to understand the space of all invariants, for any $A_{\ell,k}$; although this approach works for $A_{1,k}$, it was too messy even for $A_{2,k}$. But this work was used by [6] to prove the $A_{2,k}$ classification for $k+3$ prime. It also led to the *parity rule*, which turned out to be so important in the $A_{2,k}$ classification – this was independently discovered in [7] and [8]. In work done simultaneously but independently of [1], ref. [9] classified the *automorphism invariants* of $A_{2,k}$ (*see* equation (2.2*a* below). Ref. [8] used it, and an amazing coincide with the Fermat curves [10], to prove the $A_{2,k}$

classification for $k+3$ coprime to 6, and for $k+3=2^i$ and $k+3=3^i$. Ref. [11] used the Knizhnik-Zamolodchikov equations to find all local extensions of the A_2 chiral algebra; in our language this gives the possible ρ-couplings (*see* section 4 below). But the first and only classification of $A_{2,k}$ physical invariants for all k was given in [1]. It was done independent of – in fact obivious to – all the above work, apart from [5] (and the $A_{2,k}$ fusion rules, calculated in [12]).

Within this context, the only thing this present paper really adds is that is accomplishes the classification using only the properties (P1)-(P3). But it also simplifies and expands out more explicitly the arguments in [1], completely rewriting most of them. This should make the whole proof much more readable. It also makes explicit some results hidden inside [1]; these should be useful in other classifications – e.g. Proposition 1 is used in [13]. And unlike the proof in [1], it suggests generalization to other algebras.

The 6 outer automorphisms of $A_2^{(1)}$ are generated by C (order 2) and A (order 3). These act on the horizontal weights $(\lambda_1, \lambda_2) \in \mathcal{P}^k$ in this way:

$$C(\lambda_1, \lambda_2) = (\lambda_2, \lambda_1), \tag{1.5a}$$

$$A(\lambda_1, \lambda_2) = (n-\lambda_1-\lambda_2, \lambda_1). \tag{1.5b}$$

Note that $A^2(\lambda_1, \lambda_2) = (\lambda_2, n-\lambda_1-\lambda_2)$. The A^a are called *simple currents*, and C is called the *(charge) conjugation*. They obey the relations

$$T^{(n)}_{C\lambda, C\mu} = T^{(n)}_{\lambda\mu}, \tag{1.6a}$$

$$S^{(n)}_{C\lambda, \mu} = S^{(n)*}_{\lambda\mu}, \tag{1.6b}$$

$$T^{(n)}_{A^a\lambda, A^a\mu} = \omega^{a^2 n - at(\lambda)}\, T^{(n)}_{\lambda\mu}, \tag{1.6c}$$

$$S^{(n)}_{A^a\lambda, A^a\mu} = \omega^{bt(\lambda)+at(\mu)+nab}\, S^{(n)}_{\lambda\mu}, \tag{1.6d}$$

where $t(\lambda) = \lambda_1 - \lambda_2$ is called the *triality of* λ, and where $\omega = \exp[2\pi i/3]$. Write $\mathcal{O}$ for this 6 element group, and $\mathcal{O}\lambda$ for the orbit of λ under $\mathcal{O}$. Write $\mathcal{O}_0$ for the 3 element subgroup generated by A.

Our goal is to prove that the only level k A_2 physical invariants are:

$$\mathcal{A}_k \stackrel{\text{def}}{=} \sum_{\lambda\in\mathcal{P}^k} |\chi^k_\lambda|^2, \qquad \forall k \geq 1; \tag{1.7a}$$

$$\mathcal{D}_k \stackrel{\text{def}}{=} \sum_{\lambda\in\mathcal{P}^k} \chi^k_\lambda\, \chi^{k*}_{A^{kt(\lambda)}\lambda}, \qquad \text{for} \quad k \not\equiv 0 \pmod 3 \text{ and } k \geq 4; \tag{1.7b}$$

$$\left.\begin{array}{l}\mathcal{D}_k \overset{\text{def}}{=} \dfrac{1}{3} \displaystyle\sum_{\substack{\lambda\in\mathcal{P}^k \\ t(\lambda)\equiv 0 \,(\mathrm{mod}\, 3)}} |\chi_\lambda^k + \chi_{A\lambda}^k + \chi_{A^2\lambda}^k|^2, \\ \qquad\text{for} \quad k \equiv 0 \,(\mathrm{mod}\, 3);\end{array}\right\} \tag{1.7c}$$

$$\begin{aligned}\mathcal{E}_5 \overset{\text{def}}{=}\ & |\chi_{1,1}^5 + \chi_{3,3}^5|^2 + |\chi_{1,3}^5 + \chi_{4,3}^5|^2 + |\chi_{3,1}^5 + \chi_{3,4}^5|^2 \\ & + |\chi_{3,2}^5 + \chi_{1,6}^5|^2 + |\chi_{4,1}^5 + \chi_{1,4}^5|^2 + |\chi_{2,3}^5 + \chi_{6,1}^5|^2;\end{aligned} \tag{1.7d}$$

$$\begin{aligned}\mathcal{E}_9^{(1)} \overset{\text{def}}{=}\ & |\chi_{1,1}^9 + \chi_{1,10}^9 + \chi_{10,1}^9 + \chi_{5,5}^9 + \chi_{5,2}^9 + \chi_{2,5}^9|^2 \\ & + 2|\chi_{3,3}^9 + \chi_{3,6}^9 + \chi_{6,3}^9|^2;\end{aligned} \tag{1.7e}$$

$$\begin{aligned}\mathcal{E}_9^{(2)} \overset{\text{def}}{=}\ & |\chi_{1,1}^9 + \chi_{10,1}^9 + \chi_{1,10}^9|^2 + |\chi_{3,3}^9 + \chi_{3,6}^9 + \chi_{6,3}^9|^2 \\ & + 2|\chi_{4,4}^9|^2 + |\chi_{1,4}^9 + \chi_{7,1}^9 + \chi_{4,7}^9|^2 \\ & + |\chi_{4,1}^9 + \chi_{1,7}^9 + \chi_{7,4}^9|^2 + |\chi_{5,5}^9 + \chi_{5,2}^9 + \chi_{2,5}^9|^2 \\ & + (\chi_{2,2}^9 + \chi_{2,8}^9 + \chi_{8,2}^9)\,\chi_{4,4}^{9*} + \chi_{4,4}^9\,(\chi_{2,2}^{9*} + \chi_{2,8}^{9*} + \chi_{8,2}^{9*});\end{aligned} \tag{1.7f}$$

$$\begin{aligned}\mathcal{E}_{21} \overset{\text{def}}{=}\ & |\chi_{1,1}^{21} + \chi_{5,5}^{21} + \chi_{7,7}^{21} + \chi_{11,11}^{21} + \chi_{22,1}^{21} + \chi_{1,22}^{21} \\ & + \chi_{14,5}^{21} + \chi_{5,14}^{21} + \chi_{11,2}^{21} + \chi_{2,11}^{21} + \chi_{10,7}^{21} + \chi_{7,10}^{21}|^2 \\ & + |\chi_{16,7}^{21} + \chi_{7,16}^{21} + \chi_{16,1}^{21} + \chi_{1,16}^{21} + \chi_{11,8}^{21} + \chi_{8,11}^{21} \\ & + \chi_{11,5}^{21} + \chi_{5,11}^{21} + \chi_{8,5}^{21} + \chi_{5,8}^{21} + \chi_{7,1}^{21} + \chi_{1,7}^{21}|^2;\end{aligned} \tag{1.7g}$$

together with their *conjugations* Z^c under C, defined by:

$$(M^c)_{\lambda\mu} = M_{C\lambda,\,\mu}. \tag{1.7h}$$

Note that $\mathcal{D}_3 = \mathcal{D}_3^c$, $\mathcal{D}_6 = \mathcal{D}_6^c$, $\mathcal{E}_9^{(1)} = \mathcal{E}_9^{(1)\,c}$, and $\mathcal{E}_{21} = \mathcal{E}_{21}^c$.

The invariants equation (1.7*b*) were first found in [14], while equation (1.7*c*) was found in [15]. The exceptionals equations (1.7*d, e, g*) were found in [16], while equation (1.7*f*) was found in [2].

The remainder of this paper is devoted toward proving that equations (1.7) exhaust all A_2 physical invariants.

Sec. 2: We state here the tools which we will use to accomplish this, many of which were not yet available for [1].

Sec. 3: We find all automorphism invariants for each level k. This argument is completely rewritten and considerably shortened.

Sec. 4: For each k, we use the "parity rule" to find all weights $\lambda \in \mathcal{P}^k$ which can "couple to ρ". This is the most difficult part of the paper; it is based on sect. 4 of [1], but the arguments are given in more detail here, and the most complicated case in [1] (namely $n \equiv 2 \pmod 4$) has been completely rewritten. The arguments in this section are elementary but tedious and involve investigating several cases.

Sec. 5: Everything is put together here. This section completely rewritten and considerably simplified from sect. 5 of [1]. The main task here is to find all automorphisms of the "simple current extension" when 3 divides k.

Sect. 6: This new section explicitly handles the four anomolous levels $k = 5, 9, 21, 57$.

2. THE PARITY RULE AND OTHER TOOLS

In this section we collect together the various tools we will be using. All these apply to any rational conformal field theory, but we will state and prove only what we need. Throughout this paper we will often abbreviate "$a \equiv b \pmod c$" as "$a \equiv_c b$".

The weight ρ is very special. For one thing, there is the important property that

$$S^{(n)}_{(a,\,a),\,\lambda} = \frac{8}{\sqrt{3\,n}} \sin\left(\pi\,\frac{a\,\lambda_1}{n}\right) \sin\left(\pi\,\frac{a\,\lambda_2}{n}\right) \sin\left(\pi\,\frac{a\,(\lambda_1+\lambda_2)}{n}\right), \tag{2.1a}$$

for all $1 \le a \le \dfrac{n-1}{2}$, hence

$$S^{(n)}_{\rho\lambda} \ge S^{(n)}_{\rho\rho} > 0. \tag{2.1b}$$

Equality holds in equation (2.1*b*) iff $\lambda \in \mathcal{O}_0\,\rho$. Equation (2.1*b*) and (P3) together suggest the possibility that the values $M_{\rho\mu}$, $M_{\lambda\rho}$ may be important. Indeed this is the case: our first three lemmas given below all tell us *global* information about M, given the *local* knowledge $M_{\rho\mu}$, $M_{\lambda\rho}$.

Because $T^{(n)}$ is diagonal, equation (1.4*a*) is easy to solve: M commutes with $T^{(n)}$ iff

$$\lambda_1^2 + \lambda_1\,\lambda_2 + \lambda_2^2 \equiv \mu_1^2 + \mu_1\,\mu_2 + \mu_2^2 \pmod{3\,n}$$
$$\text{whenever } M_{\lambda\mu} \ne 0. \tag{2.1c}$$

A much harder task is to obtain useful information from equation (1.4*b*). This is the purpose of this section.

First some definitions. Call a physical invariant M a *automorphism invariant* if there exists a permutation σ of $\mathcal{P}^k$ such that

$$M_{\lambda\mu} = \delta_{\mu,\,\sigma\lambda}. \tag{2.2a}$$

For a given invariant M, let

$$\mathcal{K}_L^\mu = \{\, \lambda \in \mathcal{P}^k | M_{\lambda\mu} \neq 0 \,\}, \tag{2.2b}$$

$$\mathcal{P}_L = \{\, \lambda \in \mathcal{P}^k | \exists\, \mu \,\text{such that}\, M_{\lambda\mu} \neq 0 \,\} = \bigcup_{\mu\in\mathcal{P}^k} \mathcal{K}_L^\mu, \tag{2.2c}$$

$$\mathcal{J}_L = \{\, A^a \in \mathcal{O}_0 | A^a\, \rho \in \mathcal{K}_L^\rho \,\}, \tag{2.2d}$$

$$s_L^\lambda = \sum_{\mu\in\mathcal{P}^k} S_{\lambda\mu}^{(n)}\, M_{\mu\rho}, \tag{2.2e}$$

and define $\mathcal{K}_R^\lambda$, $\mathcal{P}_R$, $\mathcal{J}_R$ and s_R^μ similarly – e.g. $s_R^\mu = \sum_{\mu\in\mathcal{P}^k} M_{\rho\lambda}\, S_{\lambda\mu}^{(n)}$. Let $[\lambda]$ denote the orbit $\mathcal{J}_L\, \lambda$, and $[\mu]'$ denote the orbit $\mathcal{J}_R\, \mu$.

LEMMA 1. – (*a*) *Let M be any positive invariant. For each λ, $\mu \in \mathcal{P}^k$, both s_L^λ, $s_R^\mu \geq 0$. Also $s_L^\lambda > 0$ iff $\lambda \in \mathcal{P}_L$; $s_R^\mu > 0$ iff $\mu \in \mathcal{P}_R$.*

(*b*) *Let M be any physical invariant. Then $\mathcal{J}_L$ and $\mathcal{J}_R$ are groups, and so equal either $\{\, A^0 \,\}$ or $\mathcal{O}_0 = \{\, A^0,\ A^1,\ A^2 \,\}$.*

(i) *Let M be any physical. Then $M_{\lambda\mu} = M_{A^a\lambda,\, A^b\mu}$ for any $A^a \in \mathcal{J}_L$, $A^b \in \mathcal{J}_R$.*

(*d*) *Let M be a physical invariant. Suppose $M_{\lambda\rho} \leq M_{\rho\lambda}\ \forall\, \lambda \in \mathcal{P}^k$. Then $M_{\rho\lambda} = M_{\lambda\rho}\ \forall\, \lambda \in \mathcal{P}^k$ and $\mathcal{K}_L^\rho = \mathcal{K}_R^\rho$.*

(*e*) *Let M be a physical invariant, and suppose $\mathcal{K}_L^\rho = [\rho]$, $\mathcal{K}_R^\rho = [\rho]'$. Then the cardinalities $\|\mathcal{J}_L\| = \|\mathcal{J}_R\|$ are equal, so $\mathcal{J}_L = \mathcal{J}_R$, and $\mathcal{P}_L$ equals the set of all weights with zero charge with respect to $\mathcal{J}_L$,* i.e.

$$\mathcal{P}_L = \{\, \lambda \in \mathcal{P}^k | a\, t\,(\lambda) \equiv_3 0 \text{ whenever } A^a \in \mathcal{J}_L \,\}.$$

Proof. – (*a*) Evaluating $(S^{(n)}\, M)_{\lambda\rho} = (M S^{(n)})_{\lambda\rho}$ (*see* equation (1.4*b*)) gives us

$$s_L^\lambda \stackrel{\text{def}}{=} \sum_{\mu\in\mathcal{P}^k} S_{\lambda\mu}^{(n)}\, M_{\mu\rho} = \sum_{\mu\in\mathcal{P}^k} M_{\lambda\mu}\, S_{\mu\rho}^{(n)}. \tag{2.3a}$$

The RHS of equation (2.3*a*) is ≥ 0, since each $S_{\rho\mu}^{(n)} > 0$, by equation (2.1*b*), and each $M_{\mu\lambda} \geq 0$, by (P2). This gives us the first part of (*a*). In fact the RHS of equation (2.3*a*) will be > 0 iff some $M_{\lambda\mu} > 0$, *i.e.* iff $\lambda \in \mathcal{P}_L$. This gives us the second.

(*b*) From $M = S^{(n)\dagger} M S^{(n)}$ and equation (1.6*b*) we get

$$\begin{aligned} M_{A^a\rho,\,\rho} = |M_{A^a\rho,\,\rho}| &= |\sum_{\lambda,\,\mu} S^{(n)*}_{A^a\rho,\lambda}\, M_{\lambda\mu}\, S^{(n)}_{\mu\rho}| \\ &= |\sum_{\lambda,\,\mu} S^{(n)*}_{\rho\lambda}\, M_{\lambda\mu}\, S^{(n)}_{\mu\rho}\, \omega^{-at\,(\lambda)}| \\ &\leq \sum_{\lambda,\,\mu} S^{(n)*}_{\rho\lambda}\, M_{\lambda\mu}\, S^{(n)}_{\mu\rho} = M_{\rho\rho} = 1. \end{aligned} \tag{2.3b}$$

In deriving this we also used (P2) and equation (2.1*b*). Equality will happen in equation (2.3*b*) iff $a\,t\,(\lambda) \equiv_3 0$ for all $\lambda \in \mathcal{P}_L$, so (*b*) follows.

(*c*) As in (*b*), we get for any $A^a \in \mathcal{J}_L$, $A^b \in \mathcal{J}_R$,

$$\begin{aligned} M_{A^a\lambda,\,A^b\lambda\mu} &= \sum_{\lambda',\,\mu'} S^{(n)*}_{A^a\lambda,\,\lambda'}\, M_{\lambda'\mu'}\, S^{(n)}_{\mu',\,A^b\mu} \\ &= \sum_{\lambda',\,\mu'} S^{(n)*}_{\lambda\lambda'}\, M_{\lambda'\mu'}\, S^{(n)}_{\mu'\mu}\, \omega^{bt\,(\mu')-at\,(\lambda')} \\ &= \sum_{\lambda',\,\mu'} S^{(n)*}_{\lambda\lambda'}\, M_{\lambda'\mu'}\, S^{(n)}_{\mu'\mu} = M_{\lambda\mu}. \end{aligned} \tag{2.3c}$$

The third equal sign appears in equation (2.3*c*) because we learned in the proof of (*b*) that $A^a \in \mathcal{J}_L$ iff, for all $\lambda' \in \mathcal{P}_L$, $a\,t\,(\lambda') \equiv_3 0$.

(*d*) By (1.4*b*) we get

$$\begin{aligned} \sum_{\lambda\in\mathcal{P}^k} S^{(n)}_{\rho\lambda}\, M_{\lambda\rho} &= (S^{(n)}\, M)_{\rho\rho} = (M S^{(n)})_{\rho\rho} \\ &= \sum_{\lambda\in\mathcal{P}^k} M_{\rho\lambda}\, S^{(n)}_{\lambda\rho} = \sum_{\lambda\in\mathcal{P}^k} M_{\lambda\rho}\, S^{(n)}_{\lambda\rho}. \end{aligned} \tag{2.3d}$$

But by equation (2.1*b*), each $S^{(n)}_{\rho\lambda} = S^{(n)}_{\lambda\rho} > 0$. Because equality must hold in equation (2.3*d*), the desired conclusion holds.

(*e*) Each $M_{\rho\mu}$, $M_{\lambda\rho} \in \{0,\, 1\}$, by (*c*). Thus $\|\mathcal{J}_L\| = \|\mathcal{J}_R\|$ follows from (*b*), (*d*). In the proof of (*b*) we found that $\lambda \in \mathcal{P}_L$ iff λ has zero charge with respect ot all $\mathcal{J}_L$. ■

Lemma 1 was first proved in [17]. It will play an important role in section 5. Of these, (*c*) is the most important. The hypothesis in (*d*) is often satisfied, because most M have $M_{\rho\mu}$, $M_{\lambda\rho} \in \{0,\, 1\}$. In the general case (*i.e.* not A_2), we still have $\|\mathcal{J}_L\| = \|\mathcal{J}_R\|$ in (*e*), but this no longer will necessarily mean $\mathcal{J}_L = \mathcal{J}_R$. In fact, we get a more general result. Let M be any physical invariant, then for integers a, b the following three propositions are equivalent:

$M_{A^a\rho,\, A^b\rho} \neq 0$;

$a\,t(\lambda) \equiv_3 b\,t(\mu)$ whenever $M_{\lambda\mu} \neq 0$;

$M_{A^a\lambda,\, A^b\mu} = M_{\lambda\mu}\ \forall\,\lambda,\ \mu$.

This follows from the same calculation used in (*b*). It becomes particularly valuable when the algebra is semi-simple (since then there are so many simple currents).

The next lemma was proven in [7]. The only additional result here is that $\mathcal{K}_L^\rho = \{\rho\}$ iff $\mathcal{K}_R^\rho = \{\rho\}$; this follows immediately from (*d*).

LEMMA 2. – *Let M be a physical invariant. Then $\mathcal{K}_L^\rho = \{\rho\}$ iff $\mathcal{K}_R^\rho = \{\rho\}$ iff M is an automorphism invariant (*see *equation* 2.2*a*)).*

Note from equation (1.4) that the matrix product MM' of two invariants M and M' is again an invariant (at the same level). This is an important fact, and quite probably has not been exploited enough. The next lemma is the main place this property is used. It is proved using the Perron-Frobenius theory of non-negative matrices [18], and can be thought of loosely as a generalization of Lemma 2. It will be used in section 5 to significantly restrict the possibilities for the sets $\mathcal{K}_{L,R}^\lambda$ once given $\mathcal{K}_{L,R}^\rho$, and also to bound the values of $M_{\lambda\mu}$.

Any matrix M can be written as a direct sum

$$M = \bigoplus_{\ell=1}^{\alpha} B_\ell = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & B_\alpha \end{pmatrix}, \tag{2.4a}$$

of *indecomposable* submatrices B_ℓ (*i.e.* we cannot write $B_\ell = B'_\ell \oplus B''_\ell$). Let $\mathcal{I}(B_\ell)$ the indices i of M "contained" in the submatrix B_ℓ; every index i of M (in our case, every weitht $\lambda \in \mathcal{P}^k$) lies in one and only one $\mathcal{I}(B_\ell)$. We will always put $\rho \in \mathcal{I}(B_1)$. By a *non-negative martix* we mean a square matrix B with non-negative real entries. Any such matrix has a non-negative real eigenvalue $r = r(B)$ (called the *Perron-Frobenius eigenvalue* [18]) with the property that $r \geq |s|$ for all other (possibly complex) eigenvalues s of B. The number $r(B)$ has many nice properties, for example:

$$\min_i \sum_j B_{ij} \leq r(B) \leq \max_i \sum_j B_{ij}, \tag{2.4b}$$

$$\max_i B_{ii} \leq r(B); \tag{2.4c}$$

provided B is indecomposable and symmetric, either equality holds in equation (2.4*b*) iff each row sum $\sum_j B_{ij}$ is equal, and equality holds in equation (2.4*c*) iff B is the 1×1 matrix $B = (r)$. Also, there is an eigenvector v with eigenvalue r with components $v_i \geq 0$.

For example, consider the $m \times m$ matrix

$$B_{(\ell,\, m)} = \begin{pmatrix} \ell & \cdots & \ell \\ \vdots & & \vdots \\ \ell & \cdots & \ell \end{pmatrix}. \tag{2.4d}$$

Its eigenvalues are 0 (multiplicity $m-1$) and $m\,\ell$ (multiplicity 1). Therefore $r\,(B_{(\ell,\, m)}) = m\,\ell$. Its eigenvector v is $v = (1, \cdots, 1)$. These matrices $B_{(\ell,\, m)}$ have the important property that they are proportional to their square. They occur frequently in modular invariants.

LEMMA 3. – (*a*) *Let M be a positive invariant with non-zero indecomposable blocks B_ℓ, where $\rho \in \mathcal{I}\,(B_1)$. Then $r\,(B_\ell) \leq r\,(B_1)$ for all ℓ.*

(*b*) *Suppose now that $B_1^2 = r\, B_1$, for some saclar r. Then $r\,(B_\ell) = r$ for all ℓ. If in addition $B_1^T = B_1$, then each $M_{\lambda\mu} \leq r$.*

(*c*) *Now let M be a physical invariant, and $\mathcal{K}_L^\rho = [\rho]$, $\mathcal{K}_R^\rho = [\rho]'$. Suppose $M_{\lambda\mu} \neq 0$, where λ is not a fixed point of $\mathcal{J}_L$ (*i.e. *$J \in \mathcal{J}_L$ and $J\,\lambda = \lambda$ implies $J = A^0$) and μ is not a fixed point of $\mathcal{J}_R$. Then $M_{\lambda\nu} \neq 0$ iff $\nu \in [\mu]'$ and $M_{\nu\mu} \neq 0$ iff $\nu \in [\lambda]$.*

Proof. – (*a*) From $M_{\rho\rho} = (S^{(n)\dagger}\, M S^{(n)})_{\rho\rho}$ and equation (2.1*b*) we get the very crude bound

$$\max_{\lambda,\, \mu} M_{\lambda\mu} \leq \sum_{\lambda,\, \mu \in \mathcal{P}^k} M_{\lambda\mu} \leq \frac{M_{\rho\rho}}{S_{\rho\rho}^{(n)\,2}}, \tag{2.5a}$$

for any positive invariant M.

Let B be an arbitrary non-negative matrix. Looking at its Jordan block form, we see immediately that

$$\lim_{j \to \infty} (B/s)^j = 0 \qquad \text{if} \quad s > r\,(B). \tag{2.5b}$$

Moroever, $r\,((B/s)^j) = r\,(B)^j/s^j$, so (2.4*b*) tells us

$$\lim_{j \to \infty} \max_{a,\, b} ((B/s)^j)_{a,\, b} = \infty \qquad \text{if} \quad s < r\,(B). \tag{2.5c}$$

Choosing $r\,(B_1) < s < r\,(B_\ell)$ and considering $(M/s)^j$ for large j, we find from (2.5*b, c*) that we violate equation (2.5*a*).

(*b*) First note that $r = r(B_1)$, by (2.5*c*). Suppose $r(B_\ell) < r$, for some ℓ. Look at the sequence of matrices $\left(\frac{1}{r}M\right)^j$, for $j \to \infty-$ this sequence will not in general converge. However, by equation (2.5*a*) the entries of $\left(\frac{1}{r}M\right)^j$, for any j, will be bounded above by $M_{\rho\rho}/(r\, S_{\rho\rho}^{(n)\,2})$, so by Bolzano-Weierstrass the sequence $\left(\frac{1}{r}M\right)^j$ will have convergent subsequences. Let M' be the limit of any such subsequence. Clearly, M' will be a positive invariant. Suppose $r(B_\ell) < r$ for some $B_\ell \neq 0$, and let $\lambda \in \mathcal{I}(B_\ell)$. Then $\lambda \in \mathcal{P}_L(M)$ (since $B_\ell \neq 0$)), but $\lambda \notin \mathcal{P}_L(M')$ $\left(\text{because } \left(\frac{1}{r}B_\ell\right)^j \to 0 \text{ by (2.5}b\text{)}\right)$. But by hypothesis $M_{\rho\mu} = r\, M'_{\rho\mu}$ for all μ, so by Lemma 1 (*a*) we must have $\mathcal{P}_L(M) = \mathcal{P}_L(M')$ – a contradiction.

That each $M_{\lambda\mu} \leq r$ follows now by looking at MM^T : $r(MM^T) = r(B_1\, B_1^T) = r^2$, so $r^2 \geq (MM^T)_{\lambda\lambda} \geq M_{\lambda\mu}^2$ by equation (2.4*c*).

(*c*) Let $m = \|\mathcal{J}_L\|$ (which equals $\|\mathcal{J}_R\|$ by Lemma 1 (*e*)). Write out the decomposition $\oplus_\ell B_\ell$ for MM^T, as in equation (2.4*a*). Then by hypothesis, $B_1 = B_{(m,m)}$ (*see* equation (2.4*d*)), so $r(B_\ell) = m^2$ for each ℓ (by Lemma 3 (*b*)).

Now, let B_i be the block with $\lambda \in \mathcal{I}(B_i)$. Then for all $J,\ J' \in \mathcal{J}_L$, by Lemma 1 (*c*) we get

$$(B_i)_{J\lambda,\,J'\lambda} = (B_i)_{\lambda\lambda} = \sum_{\nu\in\mathcal{P}_R} M_{\lambda\nu}^2 \geq \sum_{\nu\in[\mu]'} M_{\lambda\nu}^2 = m\, M_{\lambda\mu}^2. \tag{2.5d}$$

Let B_i^λ denote the matrix

$$(B_i^\lambda)_{\nu\nu'} = \begin{cases} m\, M_{\lambda\mu}^2 & \text{if } \nu,\ \nu' \in [\lambda] \\ 0 & \text{otherwise} \end{cases}. \tag{2.5e}$$

Then element-wise, $B_i \geq B_i^\lambda$ by equation (2.5*d*), so by p. 57 of [18] we get that $r(B_i) \geq r(B_i^\lambda)$, with equality iff $B_i = B_i^\lambda$. But $B_i^\lambda = B_{(mM_{\lambda\mu}^2,\, m)}$ so $m^2 = r(B_i) \geq r(B_i^\lambda) = m^2\, M_{\lambda\mu}^2$. Therefore $M_{\lambda\mu} = 1$ and $B_i^\lambda = B_i$.

Using $M^T M$ in place of MM^T, we get the corresponding result for μ. ■

Lemma 2 is a corollary of Lemma 3 (*c*). In section 5, Lemma 3 (*b*, *c*) will be applied to the case $\mathcal{K}_L^\rho = \mathcal{K}_R^\rho = \mathcal{O}_0\,\rho$. There is a unique fixed point there: $f = (n/3,\ n/3)$. So Lemma 3 (*c*) tells us about most of the weights; the main value of Lemma 3 (*b*) for us will be in analysing the possible value of $M_{\lambda f}$, $M_{f\mu}$, but it will also be useful in section 6.

The final observation we will use is the *parity rule*. Its shortest derivation is in [19]; there is no need to repeat it here. We will only state the result, as it applies to $A_{2,k}$.

For any real numbers x, y define by $\{x\}_y$ the unique number congruent to $x \pmod{y}$ satisfying $0 \leq \{x\}_y < y$. Consider any $\lambda = (\lambda_1, \lambda_2)$, $\lambda_i \in \mathbf{Z}$, λ not necessarily in $\mathcal{P}^k$. Define the *parity* $\varepsilon(\lambda)$ of λ to be

$$\varepsilon(\lambda) = \begin{cases} 0 & \text{if } \{\lambda_1\}_n, \{\lambda_2\}_n \text{ or } \{\lambda_1+\lambda_2\}_n = 0 \\ +1 & \text{if } \{\lambda_1\}_n + \{\lambda_2\}_n < n \\ & \text{and } \{\lambda_1\}_n, \{\lambda_2\}_n, \{\lambda_1+\lambda_2\}_n > 0. \\ -1 & \text{if } \{\lambda_1\}_n + \{\lambda_2\}_n > n \\ & \text{and } \{\lambda_1\}_n, \{\lambda_2\}_n, \{\lambda_1+\lambda_2\}_n > 0 \end{cases} \tag{2.6a}$$

Then it can be shown that $\varepsilon(\lambda) \neq 0$ iff there exists a unique root lattice vector $v = \ell(2, -1) + m(1, 1)$, $\ell, m \in \mathbf{Z}$, and a unique Weyl transformation $\omega \in W(A_2)$, such that

$$(\lambda)^+ \stackrel{\text{def}}{=} \omega\lambda + nv \in \mathcal{P}^k; \tag{2.6b}$$

in this case $\varepsilon(\lambda) = \det \omega$.

LEMMA 4. – (*a*) *Let M be any invariant. Choose any $\lambda, \mu \in \mathcal{P}^k$. Then, for each ℓ coprime to* $3n$ $(\ell\lambda)\,\varepsilon(\ell\mu) \neq 0$ *and*

$$M_{\lambda\mu} = \varepsilon(\ell\lambda)\,\varepsilon(\ell\mu)\,M_{(\ell\lambda)+,\,(\ell\mu)+}. \tag{2.7}$$

(*b*) *Now let M be any positive invariant. Then for all ℓ coprime to $3n$, $M_{\lambda\mu} \neq 0$ implies $\varepsilon(\ell\lambda) = \varepsilon(\ell\mu)$.*

The more useful one for our purposes is Lemma 4 (*b*). In fact, we will be mostly interested in applying it to $\mu = \rho$. This will give us an upper bound on the sets $\mathcal{K}^{\rho}_{L,R}$, and from there Lemmas 1, 2, 3 can be used. Equation (2.7) will be used in section 6.

The parity rule is extremely powerful. For example, for the special case n coprime to 6, 4 (*b*) alone is enough to imply that $\mathcal{K}^{\lambda}_{L} \subset \mathcal{O}\lambda$, for any positive invariant M. We will not use that here (the complicated proof is given in [10]). Incidentally, a similar result holds for $A_{1,k}$, k odd – it is natural to ask how this extends to higher rank A_ℓ.

The "catch" is that proving anything using the parity rule seems to mean immersing oneself in mazes of minute details and special cases. Below is the parity rule for ρ-couplings for the A_1 modular invariant classification; it will be used in section 4 below, where we will find that the A_1 classification is embedded in some way in the A_2 one. The proof of Lemma 5, and those in section 4, look so long and complicated because we have deliberately included all details to the arguments.

Let $\mathcal{C}_L$ denote the set of all numbers coprime to L. In order to apply the parity rule, we need a systematic way of producting lots of numbers ℓ in $\mathcal{C}_L$. Fortunately, this is not difficult: for example, consider

$$\ell = \frac{L}{2^i} \pm 2^j.$$

ℓ will lie in $\mathcal{C}_{2L}$ iff either $L/2^i$ is even and $j = 0$, or $L/2^i$ is odd and $j > 0$. The reason is that these choices of i, j guarantee ℓ is odd; any other prime p dividing L will not divide $\pm 2^j$ so cannot divide ℓ. These series of ℓ's are the reason for introducing the binary expansions in equation (2.9*a*) below.

Choose any integer $m > 2$. Let $\mathcal{K}_m$ denote the set of all integers a, $0 < a < m$, satisfying:

$$\begin{cases} 0 < \{\ell\}_{2m} < m \quad \text{and} \quad \ell \in \mathcal{C}_{2m} \quad \Rightarrow \quad \{\ell a\}_{2m} < m; \\ m < \{\ell\}_{2m} < 2m \quad \text{and} \quad \ell \in \mathcal{C}_{2m} \quad \Rightarrow \quad \{\ell a\}_{2m} > m. \end{cases} \tag{2.8}$$

LEMMA 5. [2] – *Define the set $\mathcal{K}_m$ as above. Then:*

(*a*) *for* $m \neq 6, 10, 12, 30$, *we have* $\mathcal{K}_m = \{1, m-1\}$;

(*b*) $\mathcal{K}_6 = \{1, 3, 5\}$;

$\mathcal{K}_{10} = \{1, 3, 7, 9\}$;

$\mathcal{K}_{12} = \{1, 5, 7, 11\}$;

$\mathcal{K}_{30} = \{1, 11, 19, 29\}$.

Proof. – Write $m = 2^L m'$, where m' is odd. Define the integer M by $m/2 \leq 2^M < m$. First, note that $a \in \mathcal{K}_m$ iff $m - a \in K_m$. The reason is that $\ell \in \mathcal{C}_{2m}$ must be odd, so $\{\ell(m-a)\}_{2m}$ equals $m - \{\ell a\}_{2m} < m$ if $\{\ell a\}_{2m} < m$, or $3m - \{\ell a\}_{2m} > m$ if $\{\ell a\}_{2m} > m$.

Let $a \in \mathcal{K}_m$. Define $b = a/m$, so $0 < b < 1$, and write out its *binary* (= base 2) *expansion:*

$$b = 0.b_1 b_2 b_3 \ldots \stackrel{\text{def}}{=} \sum_{i=1}^{\infty} b_i 2^{-i}, \qquad b_i \in \{0, 1\}. \tag{2.9a}$$

So $b_i = 0$ means $\{2^i b\}_2 \leq 1$, while $b_i = 1$ means $\{2^i b\}_2 \geq 1$. For example, $\frac{1}{2}$ has binary expansion $0.100\ldots = 0.011\ldots$, while $\frac{1}{3} = 0.0101\ldots$.

[2] Note that this is slightly more general than Claim 1 of [1]. The proof is mostly unchanged, apart from many more details included. The proof of Lemma 5 is fortunately as bad as it gets in this paper!

Case 1 . – m is odd (*i.e.* $L = 0$). This is the simplest case. We may assume that a is odd (otherwise replace a with $m - a$). Choose j so that

$$2^{-j+1} > b \geq 2^{-j}. \tag{2.9b}$$

Put $\ell = m - 2^j$; it is coprime to $2m$. Then $\{\ell a\}_{2m} = \{m - 2^j a\}_{2m} = 3m - 2^j a > m$, because a is odd and because of equation (2.9*b*). Therefore, by equation (2.8), $\{\ell\}_{2m} > m$, which can only happen if $m - 2^j < 0$. Equation (2.9*b*) now tells us $a < 2m/2^j < 2$, *i.e.* $a = 1$.

Now, what if m is even? Putting $\ell = m - 1$ forces $a \in \mathcal{K}_m$ to be odd: for if it was even, then $\{\ell a\}_{2m} = 2m - a > m$. We may also assume $a \leq m/2$, *i.e.* $b \leq \frac{1}{2}$ (otherwise replace a with $m - a$).

Let $c = \{a/2^L\}_2$. There two different cases: either $0 < c < 1$ (to be called case 2), or $2 > c > 1$ (to be called case 3). $c \neq 0, 1$, because a is odd and $L > 0$.

Case 2 . – Define $\ell_i = m' + 2^i$. Then for $i = 1, \ldots, M - 1$, each $\ell_i \in \mathcal{C}_{2m}$, and $0 < \ell_i < m$. Then dividing equation (2.8) by m tells us that for each $1 \leq i < M$, either $c + \{2^i b\}_2 < 1$ or $2 < c + \{2^i b\}_2$: more precisely, for each $i = 1, \ldots, M - 1$,

$$\left.\begin{array}{lll} & \{2^i b\}_2 < 1 - c & \text{if } \{2^i b\}_2 < 1, \\ \text{and} & 2 - c < \{2^i b\}_2 & \text{if } \{2^i b\}_2 > 1. \end{array}\right\} \tag{2.10}$$

Choose j so that equation (2.9*b*) holds. Suppose for contradiction that $j < M$. Then by equation (2.10), $2^{j-1} b = \{2^{j-1} b\}_2 < 1 - c$, but $2^j b = \{2^j b\}_2 > 2 - c$. Hence, $2 - c < 2^j b < 2 - 2c$, *i.e.* $c < 0$, which is false.

Therefore $b < 2^{1-M}$, *i.e.* $a < m/2^{M-1} \leq 4$, so a odd implies either $a = 1$ or 3. All that remains for case 2 is to show $3 \notin \mathcal{K}_m$. We will prove this by contradiction. Note that because $c = 3/2^L < 1$, we must have $L \geq 2$; $a \leq m/2$ then means $m \geq 8$.

If $m \equiv_3 2$ use $\ell = (m+1)/3$, while if $m \equiv_3 1$ use $\ell = (m+2)/3 + m'$. If $m \equiv_9 0, 3$ take $\ell = m/3 + 1$, while if $m \equiv_9 6$ use $\ell = m/3 + 3$. In all cases $\ell \in \mathcal{C}_{2m}$, $0 < \ell < m$, but $\{\ell a\}_{2m} = 3\ell > m$, so equation (2.8) is violated. Thus $3 \notin \mathcal{K}_m$, and we are done case 2.

Case 3 . – Take $\ell_i = m' + 2^i$ and $\ell'_j = m' - 2^j$. Then for $i, j > 0$, both $\ell_i, \ell'_j \in \mathcal{C}_{2m}$. For $i = 1, \ldots, M - 1$, $0 < \ell_i < m$; for $j = 1, \ldots, M - L$, $0 < \ell'_j < m$; and for $j = M - L + 1, \ldots, M$, $-m < \ell'_j < 0$. Therefore:

$$\text{for} \quad 1 \leq i < M, \qquad 2 < \{2^i b\}_2 + c < 3; \tag{2.11a}$$

$$\text{for} \quad 1 \leq j \leq M - L, \qquad 0 < c - \{2^i b\}_2 < 1; \tag{2.11b}$$

$$\text{for} \quad M - L < j \le M, \quad \text{either } c < \{2^j b\}_2 \text{ or } 1 + \{2^j b\}_2 < c. \quad (2.11c)$$

Now suppose for some $M - L < j < M$, that $c < \{2^j b\}_2$ but $1 + \{2^{j+1} b\}_2 < c$. Then $b_j = 1$, so $\{2^{j+1} b\}_2 = 2\{2^j b\} - 2$, and we get $c < \{2^j b\}_2 < \frac{c+1}{2}$, contradicting $c > 1$. Similarly, $c < 2$ is contradicted if $1 + \{2^j b\}_2 < c$ but $c < \{2^{j+1} b\}_2$. Thus either $c < \{2^i b\}_2$ for all $M - L < i \le M$, or $1 + \{2^i b\}_2 < c$ for all $M - L < i \le M$. Moreover, if $L > 1$ then adding equation (2.11*a*) and equation (2.11*c*) with $i = j = M - 1$ tells us that if $L > 1$ then $c < \{2^i b\}_2$ iff $c < \frac{3}{2}$.

Subtracting equation (2.11*b*) from equation (2.11*a*) produces the inequality $\frac{1}{2} < \{2^i b\}_2 < \frac{3}{2}$ for all $1 \le i \le M - L$. Thus, for these i, $b_i = 0$ iff $b_{i+1} = 1$.

Summarizing, we see that the first M binary digits b_i of b are fixed by the demand that $b_1 = 0$ (since $a \le m/2$), and equations (2.11*a-c*):

$$0 = b_1 \ne b_2 \ne b_3 \ne \cdots \ne b_{M-L} \ne b_{M-L+1} = \cdots = b_M, \qquad (2.11d)$$

and for $L > 1$, $b_M = 1$ iff $c < \frac{3}{2}$. This fixes the value of b up to a correction of 2^{-M}, *i.e.* a up to $m/2^M$, so a is then completely fixed by the condition that it be odd. To eliminate this value of a (except for 7 special values of m), we will consider 5 subcases.

(i) Consider first $M - L = 1$, *i.e.* $m = 3 \cdot 2^L$, and $L > 2$ (*i.e.* $m \ne 6, 12$. Then by equation (2.11*d*) the first M binary digits of b are $b = 0.011 \cdots 1-$, where "$-$" denotes the remaining unknown digits b_i, $i > M$. Therefore $1/2 - 1/2^M \le b \le 1/2$, *i.e.* $a = m/2 - \varepsilon$ for some $0 \le \varepsilon \le m/2^M \le 2$. Therefore $a = m/2 - 1$. Since $m > 14$, $\ell = 7$ lies in $\mathcal{C}_{2m}$ and satisfies $\{\ell a\}_{2m} = \frac{3}{2} m - 7 > m$, violating equation (2.8).

(ii) Consider next $M - L = 2$, *i.e.* $m = 5 \cdot 2^L$ or $7 \cdot 2^L$, and $L > 2$ (*i.e.* $m \ne 10, 20, 14, 28$). Then $b = 0.0100 \cdots 0-$, *i.e.* $a = m/4 + \varepsilon$, for $0 \le \varepsilon \le 2$, so $a = m/4 + 1$. Then using $\ell = 7$ (if $m = 5 \cdot 2^L$) or $\ell = 5$ (if $m = 7 \cdot 2^L$) will violate equation (2.8).

(iii) Now consider $M - L > 2$, $L > 2$. The first four digits of b will be $b = 0.0101-$. If $c < \frac{3}{2}$ then putting $j = 2$ in equation (2.11*b*) gives $c > 1.01$, *i.e.* $c = 1.01-$. Now by equation (2.11*d*), $b_{M-L+1} = \cdots = b_M = 1$. Putting $i = M - L + 1$ gives $\{2^i b\}_2 + c = 1.11 - +1.01- \ge 3$, contradicting equation (2.11*a*).

If instead $c > \frac{3}{2}$, then putting $j = 1$ in equation (2.11b) gives $c = 1.10-$. Equation (2.11d) says $b_{M-L+1} = \cdots = b_M = 0$; putting $i = M - L + 1$ gives $\{\,2^i\,b\,\}_2 + c = 0.00 - +1.10- \leq 2$, contradicting equation (2.11a).

(iv) Consider next $M - L > 2$, $L = 2$. Here, either $c = 1.01 = \frac{5}{4}$ or $c = 1.11 = \frac{7}{4}$. Consider first $c = 1.01$, then $b_{M-2} = 0$, $b_{M-3} = b_{M-1} = b_M = 1$ by equation (2.11d). Putting $j = M - L - 1$, we get $c - \{\,2^j\,b\,\}_2 = 1.01 - 1.011- < 0$, contradicting equation (2.11b). If instead $c = 1.11$, then $j = M - L - 1$ gives $1.11 - 0.100- > 1$, also contradicting equation (2.11b).

(v) Finally (!), look at $M - L > 2$, $L = 1$. Then $c = \frac{3}{2}$ and $m > 16$. From equation (2.11d) we find that for M even $\frac{1}{3} - \frac{1}{3 \cdot 2^M} \leq b \leq \frac{1}{3} + \frac{2}{3 \cdot 2^M}$, and for M odd $\frac{1}{3} - \frac{2}{3 \cdot 2^M} \leq b \leq \frac{1}{3} + \frac{1}{3 \cdot 2^M}$. That is, $a = m/3 + \varepsilon$, where $-\frac{2}{3} \leq \varepsilon \leq \frac{4}{3}$ if M is even, and where $-\frac{4}{3} \leq \varepsilon \leq \frac{2}{3}$ if M is odd. So for $m \equiv_3 0$, $a_\pm = m/3 \pm 1$, and if $m \equiv_3 \pm 1$ we have $a = m/3 \mp 1/3$ respectively.

Taking $\ell = 3$ in equation (2.8) eliminates $m \equiv_3 2$: $\{\,\ell\,a\,\}_{2m} = m+1 > m$.

For $m \equiv_3 1$, take $\ell = m/2 + 6$: $\{\,\ell\,a\,\}_{2m} = \frac{10}{6}m - \frac{1}{6}m - 2 = \frac{3}{2}m - 2 > m$.

All that remains is $m \equiv_3 0$, *i.e.* $m \equiv_{36} 6, 18, 30$. For $m \equiv_{36} 6$, put $\ell = 4 + m/6$. $\ell \in \mathcal{C}_{2m}$, since $\ell \equiv_6 5$, and $\ell < m$. $\{\,\ell\,a_\pm\,\}_{2m} = \frac{4}{3}m \pm 4 + \frac{1}{3}m \pm \frac{1}{6}m = \frac{11}{6}m + 4$ or $\frac{3}{2}m - 4$, in both cases violating equation (2.8).

For $m \equiv_{36} 18$, put $\ell = 2 + m/6$. Again $\ell < m$ and $\ell \equiv_6 5$, so $\ell \in \mathcal{C}_{2m}$. $\{\,\ell\,a_\pm\,\}_{2m} = \frac{11}{6}m + 2$ or $\frac{3}{2}m - 2$, so equation (2.8) is violated.

For $m \equiv_{36} 30$, put $\ell = 6 + m/6$. Again $\ell < m$, and $\ell \equiv_6 5$, so $\ell \in \mathcal{C}_{2m}$. $\{\,\ell\,a_\pm\,\}_{2m} = \frac{11}{6}m + 6$ or $\frac{3}{2}m - 6$, so for $m > 36$ (*i.e.* $m \neq 30$), equation (2.8) is violated.

There were some special values of m that slipped through these arguments: namely $m = 6, 10, 12, 14, 20, 28, 30$. These can be worked out explicitly. ■

3. THE AUTOMORPHISM INVARIANTS

Recall the definition of automorphism invariant given in equation (2.2*a*). Let M^σ denote its coefficient matrix. In this section we will find all $A_{2,k}$ automorphism invariants.

THEOREM 1. – *The only level k automorphism invariants for A_2 are $\mathcal{A}_k$, $\mathcal{A}_k^c$ for $k \equiv_3 0$, and $\mathcal{A}_k$, $\mathcal{A}_k^c$, $\mathcal{D}_k$, $\mathcal{D}_k^c$ for $k \not\equiv_3 0$.*

That the matrix M^σ must commute with $S^{(n)}$ (*see* equation (1.4*b*)) is equivalent to

$$S^{(n)}_{\lambda\mu} = S^{(n)}_{\sigma\lambda,\,\sigma\mu}, \qquad \forall\,\lambda,\,\mu \in \mathcal{P}^k. \tag{3.1}$$

Of course, (P3) tells us $\sigma\rho = \rho$.

The first step in the proof is to constrain the "fundamental weight" (2, 1).

CLAIM 1. – $\sigma(2,\,1) \in \mathcal{O}(2,\,1)$.

Proof of Claim 1. – From equation (3.1) it suffices to show that

$$S^{(n)}_{\rho,\,\lambda} = S^{(n)}_{\rho,\,(2,\,1)} \quad \Rightarrow \quad \lambda \in \mathcal{O}(2,\,1). \tag{3.2a}$$

$S^{(n)}_{\rho,\,\lambda}$ is most conveniently evaluated using equation (2.1*a*). Since the value of $S^{(n)}_{\rho,\,\lambda}$ is constant along the orbit $\mathcal{O}\lambda$, we may suppose $\lambda_1 \le \lambda_2 \le n - \lambda_1 - \lambda_2$. We may also assume $k \ge 3$ – $k = 1,\,2$ can be verified by hand. Obviously, the only possible products

$$\sin\left(\pi\frac{a}{n}\right)\sin\left(\pi\frac{b}{n}\right)\sin\left(\pi\frac{c}{n}\right) = \sin\left(\pi\frac{1}{n}\right)\sin\left(\pi\frac{2}{n}\right)\sin\left(\pi\frac{3}{n}\right), \tag{3.2b}$$

for integers $1 \le a \le b \le c \le \frac{n}{2}$ are $(a,\,b,\,c) = (1,\,2,\,3)$, $(1,\,1,\,c)$ or $(2,\,2,\,2)$ – for any other triple the LHS of equation (3.2*b*) will clearly be larger or smaller than the RHS. In order for $a = \lambda_1$, $b = \lambda_2$, $c = \lambda_1 + \lambda_2$ or $n - \lambda_1 - \lambda_2$, these three triples require respectively $\lambda \in \mathcal{O}(2,\,1)$, $\lambda \in \mathcal{O}\rho$, or both $\lambda = (2,\,2)$ and $k = 3$. But $\lambda \in \mathcal{O}\rho$ clearly has $S^{(n)}_{\rho,\,\lambda} < S^{(n)}_{\rho,\,(2,\,1)}$. $\lambda = (2,\,2)$ at $k = 3$ can be evaluated explicitly; we find $S^{(6)}_{\rho,\,\lambda} > S^{(6)}_{\rho,\,(2,\,1)}$ has been established. ■

The claim, together with equation (2.1*c*), tells us that the only possibilities for $\sigma(2,\,1)$ are:

$$\sigma(2,\,1) \in \{\,(2,\,1),\,(1,\,2)\,\} \qquad \text{if} \quad k \equiv_3 0, \tag{3.3a}$$

$$\sigma(2,\,1) \in \{(2,\,1),\,(1,\,2),\,(k,\,2),\,(2,\,k)\} \qquad \text{if} \quad k \equiv_3 1, \tag{3.3b}$$

$$\sigma(2,\,1) \in \{(2,\,1),\,(1,\,2),\,(1,\,k),\,(k,\,1)\} \qquad \text{if} \quad k \equiv_3 2. \tag{3.3c}$$

Note that the possibilities for $k \equiv_3 0$ are realized by $\mathcal{A}_k$ and $\mathcal{A}_k^c$, respectively, and for $k \equiv_3 \pm 1$ $\mathcal{A}_k$ and $\mathcal{A}_k^c$, $\mathcal{D}_k$ and $\mathcal{D}_k^c$, respectively. Since the (matrix) product M^σ, $M^{\sigma'}$ of two automorphism invariants M^σ $M^{\sigma'}$ is another automorphism invariant $M^{\sigma'\sigma}$, to prove Theorem 1 for each k it suffices to show that the only automorphism invariant satisfying $\sigma(2,\,1) = (2,\,1)$ is $\mathcal{A}_k$.

CLAIM 2. – *Suppose for any λ, $\lambda' \in \mathcal{P}^k$, both*

$$\frac{S^{(n)}_{(2,1),\lambda}}{S^{(n)}_{\rho,\lambda}} = \frac{S^{(n)}_{(2,1),\lambda'}}{S^{(n)}_{\rho,\lambda'}} \qquad \textit{and} \qquad \frac{S^{(n)}_{(1,2),\lambda}}{S^{(n)}_{\rho,\lambda}} = \frac{S^{(n)}_{(1,2),\lambda'}}{S^{(n)}_{\rho,\lambda'}} \tag{3.4}$$

Then $\lambda = \lambda'$.

Proof of Claim 2. – The representation ring of a semi-simple complex Lie algebra is a polynomial ring freely generated by the Weyl characters of the fundamental representations (*see* Ch. VI, § 3.4, Thm. 1 of [20]). Thus the Weyl character ch_β for any highest weight $\beta \in P_+$ of A_2 can be written as a polynomial

$$ch_\beta = P_\beta\,(ch_{(1,0)},\, ch_{(0,1)}. \tag{3.5a}$$

Moreover, we know from [4] that

$$S^{(n)}_{\mu\nu}/S^{(n)}_{\rho\nu} = ch_{\mu-\rho}\left(-2\pi i\,\frac{\nu}{n}\right). \tag{3.5b}$$

Then, for any μ, $\nu \in \mathcal{P}^k$,

$$S^{(n)}_{\mu\nu}/S^{(n)}_{\rho\nu} = P_{\mu-\rho}\,(S^{(n)}_{(2,1),\nu}/S^{(n)}_{\rho,\nu},\; S^{(n)}_{(1,2),\nu}/S^{(n)}_{\rho\nu}). \tag{3.5c}$$

In particular, from equation (3.4) we find that

$$S^{(n)}_{\mu\lambda}/S^{(n)}_{\rho\lambda} = S^{(n)}_{\mu\lambda'}/S^{(n)}_{\rho\lambda'}, \qquad \forall\,\mu \in \mathcal{P}^k. \tag{3.5d}$$

Unitarity of $S^{(n)}$ now forces $\lambda = \lambda'$. ■

Now choose any $\lambda \in \mathcal{P}^k$, and put $\lambda' = \sigma\lambda$. The first equation in equation (3.4) follows from equation (3.1) and $\sigma\rho = \rho$, $\sigma(2,\,1) = (2,\,1)$. The second equation is just the complex conjugation of the first – *see* equation (1.6*b*). Thus Claim 2 tells us $\lambda = \lambda'$, *i.e.* σ is the identity.

4. THE ρ-COUPLINGS

By the set of *ρ-couplings* at level k, we mean

$$\mathcal{R}^k = \bigcup_M \mathcal{K}_L^\rho(M) = \bigcup_M \mathcal{K}_R^\rho(M),$$

the unions being over all positive invariants M of $A_{2,k}$. For example, the $A_{2,k}$ physical invariants given in equation (1.7) tell us that $\mathcal{R}^5 \supseteq \{(1,1),(3,3)\}$, $\mathcal{R}^6 \supseteq \{(1,1),(7,1),(1,7)\}$ and $\mathcal{R}^7 \supseteq \{(1,1)\}$. We learned in section 2 that the ρ-couplings should be both accessible and informative. For instance, if $\mathcal{R}^k = \{\rho\}$ then by Lemma 2 any level k physical invariant will be an automorphism invariant, and will be listed in Theorem 1.

Let $\lambda = (a, b) \in \mathcal{R}^k$. Then by equation (2.1*c*) it must satisfy

$$a^2 + ab + b^2 \equiv 3 \pmod{3n}. \tag{4.1a}$$

Another important property comes from Lemma 4 (*b*):

$$\left.\begin{array}{llll} 0 < \{\ell\} < n/2 & \text{and } \ell \in \mathcal{C}_n & \Rightarrow & \{\ell a\} + \{\ell b\} < n, \\ n/2 < \{\ell\} < n & \text{and } \ell \in \mathcal{C}_n & \Rightarrow & \{\ell a\} + \{\ell b\} > n. \end{array}\right\} \tag{4.1b}$$

Two comments about equation (4.1*b*) must be made. One is that, throughout this section, we will write $\{\cdots\}$ for $\{\cdots\}_n$. The other is that we write in equation (4.1*b*) that $\ell \in \mathcal{C}_n$ not $\ell \in \mathcal{C}_{3n}$. The reason is that for any $\ell \in \mathcal{C}_n$, there can be found an $\ell' \in \mathcal{C}_{3n}$ such that $\ell \equiv \ell' \pmod{n}$; from equation (2.6*a*) we see that $\varepsilon(\ell\lambda) = \varepsilon(\ell'\lambda)$ for any λ.

This section is devoted to a proof of the following result.

THEOREM 2. – *The only solutions to equations* (4.1) *are:*

(i) *for* $k \equiv_{12} 2, 4, 7, 8, 10, 11$*:*

$$(a, b) \in \{(1, 1)\}; \tag{4.2a}$$

(ii) *for* $k \equiv_{12} 1, 5$*:*

$$(a, b) \in \left\{(1, 1), \left(\frac{k+1}{2}, \frac{k+1}{2}\right)\right\}; \tag{4.2b}$$

(iii) *for* $k \equiv_{12} 0, 3, 6$*:*

$$(a, b) \in \{(1, 1), (1, k+1), (k+1, 1)\}; \tag{4.2c}$$

(iv) *for* $k \equiv_{12} 9$, $k \neq 21, 57$*:*

$$(a, b) \in \left\{(1, 1), (1, k+1), \left(2, \frac{k+1}{2}\right), (k+1, 1), \left(\frac{k+1}{2}, 2\right), \left(\frac{k+1}{2}, \frac{k+1}{2}\right)\right\}; \tag{4.2d}$$

(v) *for* $k = 21$ *and* $k = 57$, *resp.:*

$$(a,\ b) \in \mathcal{O}_0(1,\ 1) \cup \mathcal{O}_0(5,\ 5) \cup \mathcal{O}_0(7,\ 7) \cup \mathcal{O}_0(11,\ 11); \tag{4.2e}$$

$$(a,\ b) \in \mathcal{O}_0(1,\ 1) \cup \mathcal{O}_0(11,\ 11) \cup \mathcal{O}_0(19,\ 19) \cup \mathcal{O}_0(29,\ 29). \tag{4.2f}$$

The reason $k = 21$ and $k = 57$ are singled out here turns out be the same (*see* Lemma 5) as the reason $k = 10$ and $k = 28$ are singled out in the corresponding ρ-couplings for $A_{1,k}$. Indeed, $21 + 3 = 2(10 + 2)$ and $57 + 3 = 2(28 + 2)$. This embedding of the $A_{1,k}$ classification inside the $A_{2,2k+1}$ one remains a mystery, at least to this writer!

We will prove Theorem 2 later in the section. For now let us consider what would happen if it were true. It gives an upper bound for the sets $\mathcal{R}^k$. So for half of the levels, Theorem 2 reduces the completeness proof to the classification of the automorphism invariants, which was accomplished in Theorem 1. Theorem 2 turns out to be sufficient to complete the $A_{2,k}$ classification for all k (this is done in section 5).

CLAIM 3. – *For any* k *and any* $\lambda \in \mathcal{P}^k$, λ *satisfies the parity condition equation* (4.1*b*) *iff every* $\lambda' \in \mathcal{O}\,\lambda$ *does. Moreover, if* $\lambda = (a,\ b)$ *satisfies the condition*

$$a^2 + ab + b^2 \equiv 3 \pmod n, \tag{4.3}$$

then so will every $\lambda' \in \mathcal{O}\,\lambda$.

The proof of Claim 3 is a straightforward calculation. For example, if $\{\ell a\} + \{\ell b\} < n$, then $\{\ell n - \ell a - \ell b\} + \{\ell a\} = n - \{\ell a\} - \{\ell b\} + \{\ell a\} = n - \{\ell b\} < n$; while if $\{\ell a\} + \{\ell b\} > n$ then the same calculation gives $\{\ell n - \ell a - \ell b\} + \{\ell a\} = 2n - \{\ell b\} > n$.

Because of Claim 3, we will restrict our attention for the remainder of this section to any weight $(a,\ b) \in \mathcal{P}^k$ satisfying the parity condition equation (4.1*b*) and the norm condition equation (4.3). By Claim 3 this set of possible λ is invariant under the outer automorphisms $\mathcal{O}$. What we will actually prove is the simpler (and more general):

PROPOSITION 1. – *The set of all solutions* $\lambda \in \mathcal{P}^k$ *to equation* (4.1*b*) *and equation* (4.3), *where* $n = k + 3$, *is:*

(*a*) *for* $n \equiv_4 1, 2, 3$, $n \neq 18$*:* $\lambda \in \mathcal{O}_{0\rho}$*;*

(*b*) *for* $n \equiv_4 0$, $n \neq 12, 24, 60$*:* $\lambda \in \mathcal{O}_{0\rho} \cup \mathcal{O}_0(\rho')$, *where* $\rho' = \left(\dfrac{n-2}{2},\ \dfrac{n-2}{2}\right)$*;*

(c) *for* $n = 12, 18, 24, 60$, *respectively,* λ *lies in*

$$\mathcal{O}_0\,\rho \cup \mathcal{O}_0\,(3,\,3) \cup \mathcal{O}_0\,(5,\,5),$$
$$\mathcal{O}_0\,\rho \cup \mathcal{O}\,(1,\,4),$$
$$\mathcal{O}_0\,\rho \cup \mathcal{O}_0\,(5,\,5) \cup \mathcal{O}_0\,(7,\,7) \cup \mathcal{O}_0\,(11,\,11),$$
$$\mathcal{O}_0\,\rho \cup \mathcal{O}_0\,(11,\,11) \cup \mathcal{O}_0\,(19,\,19) \cup \mathcal{O}_0\,(29,\,29).$$

Proof of Proposition 1 *when* $n \equiv_4 0$. – We learn from the norm condition equation (4.3) that two of a, b and $n - a - b$ will be odd and one will be even; from Claim 3 we may assume for now that both a and b are odd. Let $0 < \ell < n/2$, $\ell \in \mathcal{C}_n$. Then $\ell' = \ell + n/2$ will also lie in $\mathcal{C}_n$ but will fall in the range $n/2$ to n. Then equation (4.1b) tells us

$$\{\,\ell\, a\,\} + \{\,\ell\, b\,\} < n < \{\,\ell'\, a\,\} + \{\,\ell'\, b\,\}. \tag{4.4}$$

But a is odd, so $\{\,\ell'\, a\,\} = \{\,n/2 + \ell\, a\,\}$ equals $n/2 + \{\,\ell\, a\,\}$ if $\{\,\ell\, a\,\} < n/2$, or $-n/2 + \{\,\ell\, a\,\}$ if $\{\,\ell\, a\,\} > n/2$. A similar comment applies to b. If $n/2 < \{\,\ell\, a\,\}$, then $\{\,\ell'\, a\,\} + \{\,\ell'\, b\,\} = -n/2 + \{\,\ell\, a\,\} \pm n/2 + \{\,\ell\, b\,\} \leq \{\,\ell\, a\,\} + \{\,\ell\, b\,\}$, contradicting equation (4.4); similarly with b. So $\{\,\ell\, a\,\}$, $\{\,\ell\, b\,\} < n/2$. Thus, putting $m = n/2$ we get exactly the situation stated in Lemma 5. From there we read that the only possibilities for a and b are 1 and $(n-2)/2$, unless $n = 12, 20, 24, 60$. From these we can also compute the possibilities for $n - a - b$. Equation (4.3) now reduces this list of possibilities to those given in the Proposition. ■

Thus it suffices to consider $n \equiv_4 1, 2, 3$. First we will prove two useful results.

CLAIM 4. – *For* $n \equiv_4 1, 2, 3$, *if* $a = b$ *then* $a = b = 1$.

Proof of Claim 4. – Clearly $a < n/2$, since $a + b < n$. For n even, equation (4.1b) reduces to the hypothesis of Lemma 5 with $m = n/2$, and we get $a = 1$.

Otherwise, n is odd. Let $N > 0$ be the unique integer for which $2^N < n/2 < 2^{N+1}$. Similarly, let $j \geq 0$ be the smallest integer for which $2^j\, a < n/2 < 2^{j+1}\, a$. Assume for contradiction that $a > 1$. Then $0 \leq j < N$. Take $\ell = 2^{j+1} < n/2$. Then we get $\{\,\ell\, a\,\} + \{\,\ell\, b\,\} = 2\,(2^{j+1}\, a) > n$, contradicting equation (4.1b). ■

CLAIM 5 [3].– *The greatest common divisors* $gcd\,(a,\, n)$, $gcd\,(b,\, n)$, $gcd\,(n-a-b, n) = gcd\,(a+b,\, n)$, *equal either* 1 *or* 2 (*except for* $n = 12$).

[3] The proof of this claim given in [1] was cryptic enough to have given many people problems. The statement of the claim here is actually slightly more general, since it uses only equation (4.3).

Proof of Claim 5. – By Claim 3 it suffices to prove $gcd(a, n) \leq 2$. Suppose for contradiction a prime $p \neq 2$ divides both a and n. Consider first $p = 3$. Then equation (4.3) tells us that 3 must also divide b, and that 9 cannot divide n (otherwise equation (4.3) would imply $0 \equiv_9 3$. Look at $\ell_m = 3 + mn/3$; then $\ell_1, \ell_2 \in \mathcal{C}_n$, and for $n > 18, 0 < \ell_1 < n/2 < \ell_2 < n$. However, $\{\ell_m a\} + \{\ell_m b\} = \left\{3a + mn\frac{a}{3}\right\} + \left\{3b + mn\frac{b}{3}\right\} = \{3a\} + \{3b\}$ is independent of m, so either ℓ_1 or ℓ_2 must violate equation (4.1b). (The remaining heights $n = 6, 12, 15$ can be checked by hand; only $n = 12$ turns out allow 3 to divide a.)

Now consider other primes p. By equation (4.3), $b^2 \equiv_p 3$, which has no solutions if $p \leq 7$. Let $\ell_m = 1 + mn/p$, $m = 0, 1, \ldots, p-1$. Then $\ell_m \in \mathcal{C}_n$ iff $\ell_m \not\equiv_p 0$, so except possibly for one value of m, call it m_0, each ℓ_m will lie in $\mathcal{C}_n$. Since p divides both a and n, and $0 < a < n$, we know $n \neq p$. Therefore $0 < \ell_m < n/2$ for all $0 \leq m \leq \frac{p-1}{2}$, and $n/2 < \ell_m < n$ for $\frac{p+1}{2} \leq m \leq p-1$. So from equation (4.1$b$) we get

$$\left\{b + m\frac{bn}{p}\right\} < n - a \tag{4.5a}$$

for each m satisfying $0 \leq m \leq \frac{p-1}{2}$ (except possibly $m = m_0$), and

$$\left\{b + m\frac{bn}{p}\right\} \geq n - a \tag{4.5b}$$

for each m satisfying $\frac{p+1}{2} \leq m \leq p-1$ (except possibly $m = m_0$). An "=" has been added to equation (4.5b), purely for later convenience.

Now define $b' = \left\{b + \frac{p}{2}\right\}_p - \frac{p}{2}$ $\left(\text{so } b' \equiv_p b \text{ and } -\frac{p}{2} \leq b' < \frac{p}{2}\right)$. The geometric picture: each time m is incremented by 1, $\{\ell_m b\} = \left\{b + m\frac{b'n}{p}\right\}$ changes by precisely $\frac{b'n}{p}$, unless $\ell_m b$ "crosses" an integer multiple of n, in which case $\{\ell_m b\}$ changes by $\pm n + \frac{b'n}{p}$. From this picture we can see that if each m in $m_1 \leq m \leq m_2$ satisfies equation (4.5a), then

$$|b'|\frac{n}{p}(m_2 - m_1) < n - a, \tag{4.5c}$$

unless $|b'|\frac{n}{p} > a$; similarly, if each m in $m_3 \leq m \leq m_4$ satisfies equation (4.5b), then

$$|b'|\frac{n}{p}(m_4 - m_3) < a, \tag{4.5d}$$

unless $|b'|\frac{n}{p} > n - a$. We will use equation (4.5*c, d*) to prove $|b'| \leq 1$; this would mean $b \equiv_p +1, 0, -1$, none of which can satisfy equation (4.3) (which tells us $b^2 \equiv_p 3$).

First let us eliminate the possibilities $|b'|\frac{n}{p} > a$ and $|b'|\frac{n}{p} > n - a$. The former would violate equation (4.5*d*) if we had an m such that both m and $m+1$ satisfied equation (4.5*b*) $\left(\text{since if also } |b'|\frac{n}{p} > n - a\text{, this would contradict } |b'| \leq \frac{p}{2}\right)$. But there are $\frac{p-1}{2}$ numbers between $\frac{p+1}{2}$ and $p-1$ inclusive, only one of which can equal m_0. Therefore if $\frac{p-1}{2} > 3$, *i.e.* $p > 7$, such an m will exist. Similarly, to eliminate $|b'|\frac{n}{p} > n - a$ requires that $p > 5$.

Suppose now that $0 < m_0 < \frac{p-1}{2}$, and that m_0 satisfies equation (4.5*b*). Then $\{\ell_{m_0 \pm 1} b\} < n - a \leq \{\ell_{m_0} b\}$, which forces $2|b'|\frac{n}{p} > a$ by our geometric picture. But because $p > 7$, $\frac{p+5}{2} \leq p - 1$, so $m = \frac{p+1}{2}, \frac{p+3}{2}, \frac{p+5}{2}$ all must satisfy equation (4.5*b*). Equation (4.5*d*) now tells us $2|b'|\frac{n}{p} < a$, and we get a contradiction. Thus if $0 < m_0 < \frac{p-1}{2}$, then m_0 satisfies equation (4.5*a*). The identical argument shows that if $\frac{p+1}{2} < m_0 < p - 1$, then m_0 must satisfy equation (4.5*b*).

Thus there are exactly 4 possibilities ($m_0 = 0$ cannot happen):

(i) equation (4.5*a*) holds for all $0 \leq m \leq \frac{p-1}{2}$, and equation (4.5*b*) holds for all $\frac{p+1}{2} \leq m \leq p - 1$;

(ii) $m_0 = \frac{p-1}{2}$, and m_0 satisfies equation (4.5*b*);

(iii) $m_0 = \frac{p+1}{2}$, and m_0 satisfies equation (4.5*a*);

(iv) $m_0 = p - 1$ and m_0 satisfies equation (4.5*a*).

In case (i) define $m_1 = 0$, $m_2 = \frac{p-1}{2}$; in (ii) define $m_1 = 0$, $m_2 = \frac{p-3}{2}$; in (iii) define $m_1 = 0$, $m_2 = \frac{p+1}{2}$; and in (iv) define $m_1 = -1$, $m_2 = \frac{p-1}{2}$. Then in all four cases we have equation (4.5*a*) satisfied for all $m_1 \leq m \leq m_2$, and equation (4.5*b*) satisfied for all $m_2 < m \leq p + m_1 - 1$. Then equations (4.5*c, d*) tell us $|b'|\frac{n}{p}(m_2 - m_1) < n - a$ and $|b'|\frac{n}{p}(p + m_1 - 1 - m_2 - 1) < a$. Adding these gives $|b'|\frac{n}{p}(p-2) < n$, *i.e.* $|b'| < \frac{p}{p-2} < 2$, *i.e.* $|b'| \leq 1$. But as we said this contradicts equation (4.3).

Therefore, $p = 2$ is the only prime that can divide both a and n. Since equation (4.3) shows 4 cannot divide both (since then $b^2 \equiv_4 3$, which has no integer solutions), the only possibilities for $gcd(a, n)$ are 1 or 2. ∎

Proof of Proposition 1 *for n odd.* – From Claim 3 we may assume $1 \leq a$, $b < n/2$. We need to show $a = b = 1$.

First take $\ell = (n-1)/2$; it lies in C_n and is less than $n/2$. If a is even $\{\ell a\} = n - a/2$, and if a is odd, $\{\ell a\} = n/2 - a/2$. The same applies for b. Hence $\{\ell a\} + \{\ell b\} = in + (n - a - b)/2$, where $i = 1/2, 1, 3/2$ depending on whether 0, 1 or both of a, b are even. But $i \geq 1$ contradicts equation (4.1*b*) – since as always $a + b < n$. Therefore both a and b must be odd.

Equation (4.3) tells us $\{a^2\} + \{ab\} + \{b^2\} = 3 + mn$, for some integer m. Since by definition $0 \leq \{\dots\} < n$, we have $m = 0, 1$, or 2. But $m = 2$ would imply $\{a^2\} + \{ab\} = 3 + 2n - \{b^2\} > n$, which contradicts equation (4.1*b*) with $\ell = a$ ($a < n/2$ by hypothesis, and $a \in C_n$ by Claim 5).

Next suppose $m = 1$, *i.e.*

$$\{a^2\} + \{ab\} + \{b^2\} = n + 3. \tag{4.6}$$

Choose $\ell' = (n+a)/2$, $\ell'' = (n+b)/2$ – again Claim 5 tells us these lie in C_n, and both satisfy $n/2 < \ell', \ell'' < n$. Then $\ell' a \equiv_n n/2 + a^2/2$, so $\{\ell' a\} = \{a^2\}/2 + n/2$ if $\{a^2\}$ is odd, and $\{a^2\}/2$ if $\{a^2\}$ is even. Similarly, $\{\ell' b\} = \{\ell'' a\} = \{ab\}/2 + n/2$, depending on whether $\{ab\}$ is odd or even, resp., and $\{\ell'' a\} = \{b^2\}/2 + n/2$ if $\{b^2\}$ is odd, and $\{b^2\}/2$ if $\{b^2\}$ is even. But equation (4.6) tells us that $\{a^2\}+\{ab\}+\{b^2\}$ is even, so either all three are even, or 2 are odd and 1 is even. If $\{a^2\}$ or $\{ab\}$ (or both) are even, then using ℓ' in equation (4.1*b*) gives $n < \{\ell' a\} + \{\ell' b\} \leq \{a^2\}/2 + n/2 + \{ab\}/2$, *i.e.* $n < \{a^2\} + \{ab\}$, but this contradicts equation (4.1 *b*) with $\ell = a$ chosen (by hypothesis $a < n/2$, and $a \in C_n$ by Claim 5). Similarly, if instead $\{b^2\}$ is even, then using ℓ'' in equation (4.1*b*) contradicts using b in equation (4.1*b*).

Thus $m = 0$ is forced. This requires $\{a^2\} = \{ab\} = \{b^2\} = 1$, *i.e.* $a^2 \equiv_n ab \equiv_n b^2 \equiv_n 1$; Claim 5 tells us a is invertible $(\mathrm{mod}\, n)$, so $a^2 \equiv_n ab$ implies $a \equiv_n b$, *i.e.* $a = b$. Claim 4 now forces $a = b = 1$. ∎

Proof [4] *of Proposition* 1 *for* $n \equiv_4 2$. – This is the final possibility. From equation (4.3) we get that both a and b cannot be even, so by Claim 3 we may assume a, b, are both odd, and that $a \leq b$. Then $a + b < n$ implies $a < n/2$, so $\{ a^2 \} + \{ ab \} < n$ by equation (4.1b). We want to show $a = b = 1$.

Now, exactly as in the proof for n odd, $\{ a^2 \} + \{ ab \} + \{ b^2 \} = 2n + 3$ contradicts equation (4.1b) with $\ell = a$ chosen. Also, $\{ a^2 \}+\{ ab \}+\{ b^2 \} = 3$ requires $a = b$ and hence $a = b = 1$, again exactly as in the proof for n odd.

Thus it suffices to consider the case where equation (4.6) is satisfied. Define M by $2^M < n/2 < 2^{M+1}$, so $n/2^M < 4$. As in equation (2.9a), write out the binary expansions $a/n = \sum_{i=1}^{\infty} a_i\, 2^{-i}$, $b/n = \sum_{i=1}^{\infty} b_i\, 2^{-i}$, where each a_i, $b_i \in \{0, 1\}$. Note that we cannot have all but finitely many a_i or b_i equal to 1, say (same for 0), because that would mean a/n or b/n, respectively, was a dyadic rational (*i.e.* its denominator is a power of 2) – but $n \equiv_4 2$, so this would force $a = n/2$ or $b = n/2$, which contradicts Claim 5.

Consider $\ell_i = n/2 + 2^i$, $i = 1, \ldots, M$. Then $\ell_i \in \mathcal{C}_n$, and $n/2 < \ell_i < n$, so by equation (4.1b)

$$n < \{ \ell_i\, a \} + \{ \ell_i\, b \} = \left\{ \frac{n}{2} + 2^i\, a \right\} + \left\{ \frac{n}{2} + 2^i\, b \right\}$$
$$= \{ 2^i\, a \} + \{ 2^i\, b \} + \begin{cases} n & \text{if} \quad a_{i+1} = b_{i+1} = 0 \\ 0 & \text{if} \quad a_{i+1} + b_{i+1} = 1 \\ -\,n & \text{if} \quad a_{i+1} = b_{i+1} = 1 \end{cases} \tag{4.7a}$$

The reason for equation (4.7a) is that $\{ 2^i\, a \} > n/2$ iff $a_{i+1} = 1$ (similarly for b). Now, $\{ \cdots \} < n$, so equation (4.7a) forbids $a_{i+1} = b_{i+1} = 1$, for all $i = 1, 2, \ldots, M$ (the relation $a + b < n$ forbids it for $i = 0$).

Define I by $n/2^I < b < n/2^{I-1}$, *i.e.* $b_i = 0$ for $i < I$ and $b_I = 1$. If $I - 1 > M$, then $a \leq b < 2$, *i.e.* $a = b = 1$. So we may suppose $I - 1 \leq M$.

Consider first the case $I > 1$. Then equation (4.7a) with $i = I - 1$ tells us $n < \{ 2^{I-1}\, a \} + \{ 2^{I-1}\, b \} = 2^{I-1}\, a + 2^{I-1}\, b$, *i.e.* $n/2^{I-1} < a + b$. This

[4] This argument was quite complicated in [1]; it has been completely rewritten here. This proof is more natural. The basic idea is simple: we make 4 series of numbers coprime to n out of powers of 2; writing down the equation (4.1b) inequalities for these forces either $a = b = 1$ or $n = 18$. It is the intricate and not very interesting details which make this argument so long.

is a strong inequality because the biggest $a+b$ can be is if $a_i+b_i=1$ for $I\le i\le M+1$, and $a_j=b_j=1$ for $j>M+1$: this leads to the bound $a+b<n/2^{I-1}+n/2^{M+1}$. But if instead $a_i=b_i=0$ for some $i\le M+1$, then $a+b<n/2^{I-1}+n/2^{M+1}-n/2^i-n/2^{I-1}$, contradicting the ℓ_{I-1} result. Thus $a_i+b_i=1$ is indeed forced for all $i\le M+1$: *i.e.*

$$I>1\quad\Rightarrow\quad a+b=\frac{n}{2^{I-1}}+\varepsilon,\quad \text{where } 0<\varepsilon<n/2^{M+1}<2. \tag{4.7b}$$

The case $I=1$ is identical ($\{\,2^i\,b\,\}$ is independent of b_1, for $i\ge 1$). Define $I'>1$ to be the smallest index (other than $I=1$) with $a_{I'}=1$, or $b_{I'}=1$. Again $I'-1\le M$, because otherwise $n/2<b<n/2+2$, impossible since b is odd. Then the identical argument gives

$$I=1\quad\Rightarrow\quad a+b=\frac{n}{2}+\frac{n}{2^{I'-1}}+\varepsilon,\qquad \text{where}\quad 0<\varepsilon<2. \tag{4.7c}$$

In both equations (4.7*b, c*), ε is fixed by the constraint that $a+b$ must be even. Thus we have essentially removed one degree of freedom. First we will constrain I, I'.

CLAIM 6. – $I\neq 2$. *If* $I=1$ *then* $3\le I'<M$ (*unless* $n=18$), *and*

$$\{\,ab\,\}+\{\,b^2\}=n+2,\qquad \{\,a^2\}=1. \tag{4.8}$$

Proof of Claim 6. – Suppose first that $I=2$. Then $a+b=n/2+1$, by equation (4.7*b*). From this, we can compute a^2, ab, b^2: $ab\equiv_n$, $(a+b)^2-a^2-ab-b^2\equiv_n n/2-2$; $a^2\equiv_n (a+b)\,a-ab\equiv_n a+2$; $b^2\equiv_n (a+b)\,b-ab\equiv_n b+2$. $a^2\equiv_n a+2$ tells us either $\dfrac{a\,(a-1)}{2}\equiv_n 1$ (if $a\equiv_4 3$), or $\dfrac{a\,(a-1)}{2}+\dfrac{1}{2}n\equiv_n 1$ (if $a\equiv_4 1$). Then $a\equiv_4 1$ would violate equation (4.1*b*) with $\ell=\dfrac{a-1}{2}+\dfrac{n}{2}$ $\left(\text{for then } \{\,\ell\,a\,\}=1;\ \ell\in\mathcal{C}_n \text{ because we have learned } \dfrac{a-1}{2}\in\mathcal{C}_{n/2}\right)$, so $a\equiv_4 3$. Similarly, we must have $b\equiv_4 3$, so $\dfrac{n}{2}+1=a+b\equiv_4 2$, *i.e.* $n\equiv_8 2$. Now take $\ell=\dfrac{n+2}{4}$; a, $b<n/2$ so we get $\{\,\ell\,a\,\}+\{\,\ell\,b\,\}=\left\{\dfrac{-n}{4}+\dfrac{a}{2}\right\}+\left\{\dfrac{-n}{4}+\dfrac{b}{2}\right\}=\dfrac{3\,n}{2}+\dfrac{n+2}{4}>n$, contradicting equation (4.1*b*).

Now suppose $I=1$. Then by equation (4.7*c*), $I'=2$ would violate $a+b<n$. $I=1$ means $b>n/2$, so equation (4.1*b*) gives $\{\,ab\,\}+\{\,b^2\,\}>n$. But by equation (4.6), and the fact that both $\{\,ab\,\}$ and $\{\,b^2\,\}$ must be odd, we get equation (4.8).

If $I' \geq M$, then $a < n/2^{I'-1} \leq n/2^{M-I} < 8$, and $n/2 < b < n/2+8$, which give us the possibilities $a = 1, 3, 5$ or 7, and $b = n/2+2$, $n/2+4$, or $n/2+6$. But for $a = 3, 5, 7$ respectively, the condition $\{a^2\} = 1$ means n must divide 8, 24 and 48. $(a, b) = (1, n/2+2)$ means $2 \equiv_n ab + b^2 \equiv_n n/2+2+n/2+4$, *i.e.* n divides 4. $(a, b) = (1, n/2+4)$ means $2 \equiv_n n/2+4+n/2+16$, *i.e.* n divides 18. $(a, b) = (1, n/2+6)$ means $2 \equiv_n n/2+6+n/2+36$, *i.e.* n divides 40.

But $n > 3$ and $n \equiv_4 2$, so the n which must be explicitly checked are $n = 6, 10, 18$. ■

Now that the know so much about a, b and $a+b$, a similar game can be played with them. In particular, define $\ell'_i = \{n/2 + 2^i a\}$, $\ell''_i = \{n/2+2^i b\}$, and $\ell'''_j = \{n/2+2^j(a+b)\}$. Note that from Claim 5 these lie in $\mathcal{C}_n$ for $i \geq 1$ and $j \geq 0$.

Define the binary digits $(a^2)_i$, $(ab)_i$, $(b^2)_i$, $(a^2+ab)_i$, and $(ab+b^2)_i$, by $\{a^2\}/n = \sum_{i=1}^{\infty} (a^2)_i\, 2^{-i}$, etc. Then the identical calculation which led to equation (4.7a) gives us

$$\{\ell'_i a\} + \{\ell'_i b\} = \{2^i a^2\} + \{2^i ab\} + \begin{cases} n & \text{if} \quad (a^2)_{i+1} = (ab)_{i+1} = 0 \\ 0 & \text{if} \quad (a^2)_{i+1} + (ab)_{i+1} = 1; \\ -n & \text{if} \quad (a^2)_{i+1} = (ab)_{i+1} = 1 \end{cases} \tag{4.9}$$

with similar expressions for ℓ''_i and ℓ'''_j (for ℓ''_i, replace a^2 and ab in equation (4.9) with ab and b^2; for ℓ'''_j replace them with a^2+ab and $ab+b^2$). Moreover, when $I > 1$, we know $a_i = 0 = b_i$ for $1 \leq i < I$, and $a_i + b_i = 1$ for $I \leq i \leq M+1$; also equation (4.7 b) tells us $(a+b)_i = 0$ for all $1 \leq i \leq M+1$, except $(a+b)_{I-1} = 1$. This means: ℓ'_i, $\ell''_i > n/2$ for $1 \leq i \leq I-2$; for each $I-1 \leq i \leq M$ either $\ell'_i < n/2 < \ell''_i$ or $\ell''_i < n/2 < \ell'_i$; for $0 \leq j \leq M$, $\ell'''_j > n/2$, except for $\ell'''_{I-2} < n/2$. From equation (4.1b), these inequalities tell us how the quantities like equation (4.9) compare to n, for all $1 \leq i \leq M$ and $0 \leq j \leq M$.

For $I = 1$, the identical inequalities hold for ℓ'_i, ℓ''_i, except with I there replaced with I' here. The same applies to ℓ'''_j, except for the additional change that $\ell'''_0 < n/2$.

Consider now $I \geq 3$. Since $a < n/2$, we have $\{a^2+ab\} = \{a^2\}+\{ab\}$; since $b < n/2$ we have $\{ab+b^2\} = \{ab\} + \{b^2\}$. Note that induction on i gives us

$$(a^2+ab)_i + (ab+b^2)_i = 1 \quad \text{for all } 1 \leq i \leq I-2 \tag{4.10a}$$

(both equal to 0 would contradict $\{ a^2+ab \} = \{ ab+b^2 \} = n+3+\{ ab \} > n$; both 1 would contradict equation (4.1b) with ℓ'''_{i-1}. Then equation (4.1b) with ℓ'''_{I-2} forces

$$(a^2 + ab)_{I-1} = (ab + b^2)_{I-1} = 1, \tag{4.10b}$$

because the alternative, namely $(a^2 + ab)_{I-1} + (ab + b^2)_{I-1} = 1$, leads to

$$\begin{aligned} n &> \{ 2^{I-2} (a^2 + ab) \} + \{ 2^{I-2} (ab + b^2) \} \\ &= 2 \{ 2^{I-3} (a^2 + ab) \} - n + 2 \{ 2^{I-3} (ab + b^2) \} \\ &> 2n - n = n, \end{aligned} \tag{4.10c}$$

a contradiction (the first inequality is the ℓ'''_{I-2} condition, the second ℓ'''_{I-3}). And now, by the identical argument which gave us equation (4.7a), we find that there exists an $I_0 \geq I$ such that

$$\left. \begin{aligned} n + 3 + \{ ab \} = \{ a^2 + ab \} + \{ ab + b^2 \} = n + \frac{n}{2^{I_0 - 1}} + \varepsilon, \\ 0 < \varepsilon < \frac{n}{2^{M+1}} < 2. \end{aligned} \right\} \tag{4.10d}$$

$\Big($$I_0$ is the first index $\geq I$ such that $(a^2+ab)_{I_0}+(ab+b^2)_{I_0} \geq 1-I_0 \leq M+1$ since otherwise $n + 3 < \{ a^2 + ab \} + \{ ab + b^2 \} < n + \frac{n}{2^{M+1}} + \frac{n}{2^{M+1}} < n + 4$, an impossibility.$\Big)$

We can now fix I. To do this, note that the ℓ'_i conditions tell us that either

$$\{ a^2 \} + \{ ab \} = \frac{n}{2^{I_1 - 1}} + \varepsilon' \qquad \text{for} \quad 0 < \varepsilon' < \frac{n}{2^{I-1}}, \tag{4.11a}$$

or

$$\{ a^2 \} + \{ ab \} = \frac{n}{2} + \frac{n}{2^{I_1 - 1}} + \varepsilon' \qquad \text{for} \quad 0 < \varepsilon' < \frac{n}{2^{I-1}}, \tag{4.11b}$$

for some $I_1 > 1$ in equation (4.11a) and $I_2 > 2$ in equation (4.11b) (if $(a^2)_i+(ab)_i \geq 1$ for some $1 < i \leq I-1$, the derivation is identical to that of equation (4.7), using ℓ'_i in place of ℓ_i; otherwise $\{ a^2 \}$, $\{ ab \} < n/2^{I-1}$, so equation (4.11) will be satisfied for some $I_1 \geq I$). The identical expressions apply to $\{ ab \} + \{ b^2 \}$, of course, using ℓ''_i – call its parameters I_2 and ε''. But according to equation (4.11), equation (4.10b) can be satisfied iff

$I_1 = I = I_2$. But then equation (4.11) says equation (4.10*a*) can be satisfied iff there are no i between 1 and $I-1$ – *i.e.* $I=3$.

So $I=3$ is forced. Equation (4.7*a*) then reads $a+b = n/4+\varepsilon'''$, where $0<\varepsilon'''<2$ is fixed by $a+b$ being even. From $3+\{ab\} \equiv_n (a+b)^2$ we get

$$3+\{ab\} = \begin{cases} (7n+18)/8 & \text{if} \quad n \equiv_{16} 2 \\ (5n+2)/8 & \text{if} \quad n \equiv_{16} 6 \\ (3n+18)/8 & \text{if} \quad n \equiv_{16} 10 \\ (n+2)/8 & \text{if} \quad n \equiv_{16} 14 \end{cases} \tag{4.12}$$

Equation (4.10*d*) is compatible with equation (4.12) only if $n \equiv_{16} 14$. In this case we can compute $\{b^2\}$ as we did in Claim 6, and we find $\{b^2\} = \frac{1}{8}n + \frac{b}{2} + \frac{11}{4}$ (if $b \equiv_4 1$) or $\frac{5}{8}n + \frac{b}{2} + \frac{11}{4}$ (if $b \equiv_4 3$). In either case (at least for $n > 14$), taking ℓ_2'' gives us $n - 11 + 2b + 11 > n$, which contradicts equation (4.1*b*) ($I=3$ here, so $\ell_2'' < n/2$).

Finally, consider the remaining possibility: $I=1$ and $M > I' \geq 3$. $\ell_0''' < n/2$, but $(ab+b^2)_1 = 0$ by equation (4.8), so $(1+ab)_1 = 1$, *i.e.* $\{ab\}+1 > n/2$, so $\{ab\} \geq n/2+2$ (it must be odd, and coprime to n).

Define $J > 1$ by $n/2+n/2^J < \{ab\} < n/2+n/2^{J-1}$, and suppose for contradiction that $J < I'$. Then as in equation (4.7*b*) derivation (with ℓ_i' in place of ℓ_i) we get $1+\{ab\} = n/2+n/2^{J-1}+\varepsilon$, $0<\varepsilon<1$. That is, $(a^2+ab)_i = 0$ for all $i \leq M+1$, except for $i=1$ and $i=J-1$. But by equation (4.8), $(ab+b^2)_i = 0$ for all $i \leq M$. Now, $\ell_{I'-2}''' < n/2$ produces a contradiction in equation (4.1*b*): $(a^2+ab)_{I'-1} = 0 = (ab+b^2)_{I'-1}$, since $J < I'$ by hypothesis.

Thus $I' \leq J$. If we had $\{b^2\} > n/2$ then this would give us $n+2 = \{ab\}+\{b^2\} > n/2+2+n/2 = n+2$, a contradiction.

Therefore $(b^2)_1 = 0$. As in equation (4.10*a*), the constraints $\{ab\} + \{b^2\} > n$ and equation (4.1*b*) with ℓ_{i-1}'' tell us $(ab)_i + (b^2)_i = 1$ for $i = 2, \ldots, I'-1$. As in equation (4.10*b*), we also get $(ab)_{I'} = (b^2)_{I'} = 1$. Now $n+2 = \{ab\}+\{b^2\}$ implies $(ab)_i = (b^2)_i = 0$ for $I' < i \leq M$. Also, $(a^2)_i = 0$ for all $i \leq M+1$. But either $\ell_{I'}'$ or $\ell_{I'}''$ will be less than $n/2$ – whichever is will violate equation (4.1*b*). ■

5. THE SIMPLE-CURRENT CHIRAL EXTENSION

In this section we use Theorem 2 to find the possible values $M_{\rho\mu}$, $M_{\lambda\rho}$ for most k. We will find that except possibly for four values of k

considered in the next section, a physical invariant will necessarily either be a automorphism invariant, or an automorphism of the *simple-current chiral extension.* The former are listed in Theorem 1; the latter are given in Theorem 3 below. This will complete the classification of $SU(3)_k$ for all $k \neq 5, 9, 21, 57$.

CLAIM 7. – *Let M be a level $k = n - 3$ physical invariant. Let $\rho' = (n/2 - 1, n/2 - 1)$. Then for each $\lambda \in \mathcal{P}^k$, $M_{\rho\lambda} = M_{\lambda\rho} \in \{0, 1\}$. $\mathcal{R} \stackrel{\text{def}}{=} \mathcal{K}_L^\rho = \mathcal{K}_R^\rho$ will equal one of the following sets:*

(a) for $n \equiv_3 1, 2$, $n \neq 8$, $\mathcal{R}$ will equal $\{\rho\}$;

(b) for $n \equiv_3 0$, $n \neq 12, 24$, $\mathcal{R}$ will equal either $\{\rho\}$ or $\mathcal{O}_0\,\rho = \{\rho, A_\rho, A^2\rho\}$;

(c) for $n = 8$, $\mathcal{R}$ will either equal $\{\rho\}$ or $\{\rho, \rho'\}$;

for $n = 12$, $\mathcal{R}$ will equal either $\{\rho\}$, $\mathcal{O}_0\,\rho$, or $\mathcal{O}_0\,\rho \cup \mathcal{O}_0\,\rho'$;

for $n = 24$, $\mathcal{R}$ will either equal $\{\rho\}$, $\mathcal{O}_0\,\rho$, or $\mathcal{O}_0\,\rho \cup \mathcal{O}_0\,\rho' \cup \mathcal{O}_0\,\rho'' \cup \mathcal{O}_0\,\rho'''$, where $\rho'' = (5, 5)$ and $\rho''' = (7, 7)$.

Proof for $n \neq 8, 12, 24, 60$. – We will defer the proof of Claim 7 for the heights $n = 8, 12, 24, 60$ to the next section.

Claim 7 is automatic for $n \equiv_{12} 1, 2, 5, 7, 10, 11$, by Theorem 2 and (P3). For the other levels, we will show $\mathcal{K}_L^\rho$ must equal one of the given possibilities, and also that each $M_{\lambda\rho} \in \{0, 1\}$. By symmetry the same comments apply to $\mathcal{K}_R^\rho$ and $M_{\rho\lambda}$, so $M_{\rho\lambda} = M_{\lambda\rho}$ and $\mathcal{K}_L^\rho = \mathcal{K}_R^\rho$ then follow from Lemma 1 (*d*).

Consider $n \equiv_{12} 4, 8$. Theorem 2 tells us $\mathcal{K}_L^\rho \subseteq \{\rho, \rho'\}$. $\rho = \rho'$ for $n = 4$, so we may assume $n > 8$ here. We may assume $1 \leq m \stackrel{\text{def}}{=} M_{\rho'\rho}$ (otherwise $\mathcal{K}_L^\rho = \{\rho\}$ and we are done). Then (*see* Lemma 1 (*a*))

$$\begin{aligned} 0 \leq s_L^{(1,2)} &= S^{(n)}_{(1,2),\rho} \cdot 1 + S^{(n)}_{(1,2),\rho'} \cdot m \\ &= \frac{2}{\sqrt{3}\,n}\{(1+m)\sin[2\pi/n] + (1-m) \\ &\qquad \times \sin[4\pi/n] - (1+m)\sin[6\pi/n]\} \\ &\leq \frac{2}{\sqrt{3}\,n}(1+m)\{\sin[2\pi/n] - \sin[6\pi/n]\}. \end{aligned} \tag{5.1}$$

For $n > 8$, the RHS of equation (5.1) is negative. Therefore, for $n > 8$ $M_{\rho'\rho} = 0$ so $\mathcal{K}_L^\rho = \{\rho\}$.

Now suppose $n \equiv_3 0$, and $\{\rho\} \neq \mathcal{K}_L^\rho \subseteq \mathcal{O}_0\,\rho$. Then Lemma 1 (*b*) says $M_{A\rho,\,\rho} \neq 0$ iff $M_{A^2\rho,\,\rho} \neq 0$, so $\mathcal{K}_L^\rho = \mathcal{O}_0\,\rho$. Lemma 1 (*c*) now tells us $1 = M_{\rho\rho} = M_{A\rho,\,\rho} = M_{A^2\rho,\,\rho}$.

All that remains is $n \equiv_{12} 0$, where Theorem 2 tells us $\mathcal{K}_L^\rho \subseteq \mathcal{O}_0\,\rho \cup \mathcal{O}_0\,\rho'$. Define $m = \sum_{i=0}^{2} M_{A^i\rho,\,\rho}$ and $m' = \sum_{i=0}^{2} M_{A^i\rho',\,\rho}$ – we may suppose $m' \geq 1$ (otherwise $\mathcal{K}_L^\rho \subseteq \mathcal{O}_0\,\rho$, which was done in the previous paragraph). We will first prove that $m \leq m'$. There are two cases to consider: by Lemma 1 (*b*) either $\mathcal{J}_L = \{A^0\}$ or $\{A^0,\, A,\, A^2\}$. In the first case $m = 1$ by (P3), so by supposition $m \leq m'$. For the second case, Lemma 1 (*c*) tells us $m = 3\,M_{\rho\rho} = 3$ and $m' = 3\,M_{\rho'\,\rho} \geq 3$, so again $m \leq m'$.

Then, by Lemma 1 (*a*) again and by equation (1.6*d*), we have

$$
\begin{aligned}
0 \leq s_L^{(1,4)} &= S^{(n)}_{(1,4),\,\rho} \cdot m + S^{(n)}_{(1,4),\,\rho'} \cdot m' \\
&= \frac{2}{\sqrt{3}\,n} \{ (m+m') \sin[2\pi/n] + (m-m') \sin[8\pi/n] \\
&\quad - (m+m') \sin[10\pi/n] \} \\
&\leq \frac{2}{\sqrt{3}\,n} (m+m') \{ \sin[2\pi/n] - \sin[10\pi/n] \}. \qquad (5.2)
\end{aligned}
$$

But the RHS of equation (5.2) will be negative unless $n = 12$. ■

When $\mathcal{R} = \{\rho\}$, Lemma 2 tells us M will be listed in Theorem 1. We will handle the anomolous ρ-couplings of $n = 8$, 12, 24, or 60 in section 6; here we consider $n \equiv_3 0$ and $\mathcal{R} = \mathcal{O}_0\,\rho$ – this corresponds to a simple-current chiral extension. But first let us review what we know.

Recall the definition of *triality*: $t(\lambda) \equiv_3 \lambda_1 - \lambda_2$. Let $\mathcal{P}_0$ denote the set of all weights $\lambda \in \mathcal{P}^k$ with $t(\lambda) \equiv_3 0$, and $\mathcal{P}_{[]} = \mathcal{P}_0/\mathcal{O}_0$ be the set of all orbits $[\lambda] = \mathcal{O}_0\,\lambda \subset \mathcal{P}_0$. Lemma 1 (*e*) tells us $\mathcal{P}_L = \mathcal{P}_R = \mathcal{P}_0$. Note that there is only one "fixed point" of $\mathcal{O}_0$, namely $f = (n/3,\, n/3)$. Lemma 3 (*c*) defines a mapping σ with a domain and range contained in $\mathcal{P}_{[]} \sim \{f\}$, with the property that when $\lambda,\, \mu \neq f$, then $M_{\lambda\mu} \neq 0$ iff $M_{\lambda\mu} = 1$ iff $[\mu] = \sigma[\lambda]$. So we already know a considerable amount about M. All that remains is to understand what M looks like at the fixed point f, and then to find σ. That f can cause complications is apparent by looking at the exceptional $\mathcal{E}_9^{(2)}$.

THEOREM 3. – *Suppose* $\mathcal{R}(M) = \mathcal{O}_0\,\rho$. *Then* M *is either the simple-current invariant* $\mathcal{D}_k$ *given in equation* (1.7*c*), *its conjugation* $\mathcal{D}_k^c$, *the exceptional* $\mathcal{E}_9^{(2)}$ *given in equation* (1.7*f*), *or its conjugation* $\mathcal{E}_9^{(2)\,c}$.

Proof. – *Step* 1: We begin by investigating $M_{f\lambda}$, $M_{\lambda f}$.

Look at the decomposition $\oplus_i B_i$ of MM^T, and $\oplus_j B'_j$ of $M^T M$ (*see* equation (2.4*a*)), where $\rho \in \mathcal{I}(B_1) \cap \mathcal{I}(B'_1)$ and $f \in \mathcal{I}(B_2) \cap \mathcal{I}(B'_2)$. Now, $B_1 = B'_1 = B_{(3,3)}$ (*see* equation (2.4*d*)), so by Lemma 3 (*b*) $r(B_2) = r(B'_2) = 9$. One thing this means is (*see* equation (2.4*c*))

$$(B_2)_{ff} = \sum_{\mu} M_{f\mu}^2 = M_{ff}^2 + 3 \sum_{[\mu]\neq[f]} M_{f\mu}^2 \leq 9. \tag{5.3}$$

Let $[\lambda^1]$, $[\lambda^2]$, ... denote the different orbits $[\lambda] \subset \mathcal{K}_R^f \sim \{f\}$, and $[\mu^1]$, $[\mu^2]$, $\cdots \subset \mathcal{K}_R^f \sim \{f\}$. From equation (5.3) we read off that $M_{\lambda^i f} = 1 = M_{f\mu^j}$ for all i, j.

Step 2: Now, look at the commutation relations that σ and λ^i must satisfy. First, choosing $\mu \notin \mathcal{K}_R^f$, $\mu \neq f$, and any $\lambda^i \neq f \in \mathcal{K}_L^f$, we get

$$S_{f\mu}^{(n)} = \sum_{\nu\in\mathcal{P}^k} M_{\lambda^i\nu} S_{\nu\mu}^{(n)} = \sum_{\nu\in\mathcal{P}^k} S_{\lambda^i\nu}^{(n)} M_{\nu\mu} = 3\, S_{\lambda^i,\sigma^{-1}\mu}^{(n)}, \tag{5.4a}$$

where by "$\sigma^{-1}\mu$" in equation (5.4*a*) we mean any element of $\sigma^{-1}[\mu]$ – because $\lambda^i \in \mathcal{P}_0$, equation (1.6*d*) tells us the RHS of equation (5.4*a*) is unaffected by this choice.

We may assume $n > 6$ (for $n = 6$, equation (2.1*c*) alone is enough to force the partition function to be $\mathcal{D}_3 = \mathcal{D}_3^c$). Thus $(2,\,2) \neq f$. Now $(2,\,2) \in \mathcal{K}_L^f$ only if $3\, S_{(2,2),\rho}^{(n)} = S_{f\rho}^{(n)}$ using equation (5.4*a*), *i.e.* only if

$$\sin\left(\frac{2\pi}{n}\right)\sin\left(\frac{2\pi}{n}\right)\sin\left(\frac{4\pi}{n}\right) = \frac{\sqrt{3}}{8}, \tag{5.4b}$$

using equation (2.1*a*). But the LHS is a strictly decreasing function of $n \geq 9$, so equality there can only happen for one value of n. It turns out $n = 12$ is this value. Therefore, for $n \neq 12$, $(2,\,2) \in \mathcal{K}_L^f \cup \mathcal{K}_R^f$.

Similarly, for $n \neq 12$, $(4,\,1) \notin \mathcal{K}_L^f \cup \mathcal{K}_R^f$ and $(1,\,4) \notin \mathcal{K}_L^f \cup \mathcal{K}_R^f$.

Step 3: The weights (2, 2), (1, 4) and (4, 1) will play the role here that (2, 1) and (1, 2) did in Section 3. We are interested then in the possibilities for $[\mu'] \stackrel{\text{def}}{=} \sigma[(2,\,2)]$ and $[\mu''] \stackrel{\text{def}}{=} \sigma[(4,\,1)]$.

The equation $MS^{(n)} = S^{(n)}M$ evaluated at $((2,\,2),\,\rho)$ and $((4,\,1),\,\rho)$ give us

$$3\, S_{\mu'\rho}^{(n)} = 3\, S_{(2,2),\rho}^{(n)}, \tag{5.5a}$$

$$3\, S_{\mu''\rho}^{(n)} = 3\, S_{(4,1),\rho}^{(n)}. \tag{5.5b}$$

But the same argument used in the proof of Claim 1 tells us that for $n \geq 9$ and divisible by 3, the only possibilities for $\mu' \in \mathcal{P}_0 \sim f$ satisfying equation (5.5*a*) are $[\mu'] = [(2,\,2)]$, $[(4,\,1)]$ and $[(1,\,4)]$, and for $n \geq 12$ and divisible by 3, the only possibilities for $\mu'' \in \mathcal{P}_0 \sim f$ satisfying equation (5.5*b*) are $[\mu''] = [(2, 2)], [(4, 1)], [(1, 4)]$, and $[(3, 3)]$. $[\mu''] = [(3, 3)]$ is ruled out by the inequality

$$\sin(x) \sin(y) \leq \sin\left(\frac{x+y}{2}\right)$$
$$\text{whenever } 0 < x, \quad 0 < y, \quad x + y < \pi, \tag{5.6a}$$

which is proven by simple calculus. The possibility $S^{(n)}_{\rho,(2,2)} = S^{(n)}_{\rho,(4,1)}$ reduces to

$$0 = 1 - 16 \sin^2\left(\frac{\pi}{n}\right) + 16 \sin^4\left(\frac{\pi}{n}\right), \tag{5.6b}$$

which has exactly one relevant solution: $n = 12$. The result is that, for all n divisible by 3 (except possibly $n = 12$), equation (5.5*a*) forces $\sigma[(2, 2)] = [(2, 2)]$, and equation (5.5*b*) forces $\sigma[(4, 1)] = [(4, 1)]$ or $[(1, 4)]$.

We may assume, replacing M with MC if necessary, that $\sigma[(4, 1)] = [(4, 1)]$. Then the commutation of M with $C = S^2$ forces $\sigma[(1, 4)] = [(1, 4)]$.

Step 4: By the representation ring argument in Claim 2, we find that the Weyl character ch_β for any weight $\beta \in A_2^*$ with $t(\beta) \equiv_3 0$, can be expressed as a polynomial in $ch_{(1,1)}$, $ch_{(0,3)}$, and $ch_{(3,0)}$. The reason is that any such weight can be written as a linear combination over non-negative integers of (1, 1), (0, 3) and (3, 0), and also that any A_2 root α obeys $t(\alpha) \equiv_3 0$ (so the dominant descendants of weights in $\mathcal{P}_0 - \rho$ will also lie in $\mathcal{P}_0 - \rho$). Thus for any $\lambda, \mu \in \mathcal{P}_0$, there exists a polynomial P_λ such that

$$\frac{S^{(n)}_{\lambda\mu}}{S^{(n)}_{\rho\mu}} = P_\lambda\left(\frac{S^{(n)}_{(2,2),\mu}}{S^{(n)}_{\rho\mu}}, \frac{S^{(n)}_{(1,4),\mu}}{S^{(n)}_{\rho\mu}}, \frac{S^{(n)}_{(4,1),\mu}}{S^{(n)}_{\rho\mu}}\right). \tag{5.7}$$

This equation has two major consequences for us.

The first is, let $\lambda^i \in \mathcal{K}_L^f \sim f$, then by equation (5.4*a*) we obtain

$$\left.\begin{aligned} \frac{S^{(n)}_{(2,2),f}}{S^{(n)}_{\rho f}} &= \frac{3\,S^{(n)}_{(2,2),\lambda^i}}{3\,S^{(n)}_{\rho\lambda^i}} = \frac{S^{(n)}_{(2,2),\lambda^i}}{S^{(n)}_{\rho\lambda^i}}, \\ \frac{S^{(n)}_{(4,1),f}}{S^{(n)}_{\rho f}} &= \frac{3\,S^{(n)}_{(4,1),\lambda^i}}{3\,S^{(n)}_{\rho\lambda^i}} = \frac{S^{(n)}_{(4,1),\lambda^i}}{S^{(n)}_{\rho\lambda^i}}. \end{aligned}\right\} \tag{5.8a}$$

By the argument in Claim 2, equations (5.7) and (5.8*a*) together force

$$S^{(n)}_{\mu f} / S^{(n)}_{\rho f} = S^{(n)}_{\mu\lambda^i} / S^{(n)}_{\rho\lambda^i}, \qquad \forall\, \mu \in \mathcal{P}_0. \tag{5.8b}$$

Multiplying equation (5.8b) by $S_{\mu f}^{(n)*}$ (which vanishes when $\mu \notin \mathcal{P}_0$) and summing over $\mu \in \mathcal{P}^k$, this forces the contradiction $\lambda^i = f$. This means $M_{\lambda f} = M_{f\lambda} = 3\,\delta_{f\lambda}$ (the value "3" here is fixed by Lemma 3 (b)).

The other major consequence of equation (5.7) is the following. Choose any λ, $\mu \in \mathcal{P}_0 \sim f$. Then $MS^{(n)} = S^{(n)}M$ tells us

$$3\,S_{\lambda\mu}^{(n)} = 3\,S_{\sigma\lambda,\,\sigma\mu}^{(n)}. \tag{5.9a}$$

Thus again from equation (5.7) and the facts that $\sigma[\lambda] = [\lambda]$ for $\lambda = \rho$, (2, 2), (1, 4), (4, 1), we find

$$S_{\lambda\mu}^{(n)}/S_{\rho,\,\mu}^{(n)} = S_{\lambda,\,\sigma\mu}^{(n)}/S_{\rho,\,\sigma\mu}^{(n)}, \qquad \forall\,\lambda \in \mathcal{P}_0, \quad \forall\,\mu \in \mathcal{P}_0 \sim f. \tag{5.9b}$$

Multiplying this by $S_{\lambda\mu}^{(n)*} + S_{\lambda,\,A\mu}^{(n)*} + S_{\lambda,\,A^2\mu}^{(n)*}$ (which vanishes for $\lambda \notin \mathcal{P}_0$) and summing over $\lambda \in \mathcal{P}^k$, we get $\sigma\mu \in [\mu]$.

Thus $M = \mathcal{D}_k$. ■

6. THE EXCEPTIONAL LEVELS

The analysis in the last section avoided four heights: $n = 8$, 12, 24 and 60. There are various ways we can handle these. One way is the lattice method, employed in [21]. But this is a bit of overkill: that method finds much more than just the physical invariants. The consequence is that, for higher levels (or higher ranks), the lattice method becomes unfeasible. For example, it has never been worked out for $n = 60$.

The methods developed in this paper however also work for these exceptional levels – they merely require a bit more effort. That will be the task in this section: to complete the $A_{2,\,k}$ classification for these four levels. The first thing to do is to complete the proof of Claim 7 for these levels.

Proof of Claim 7 *for* $n = 8$, 12, 24, 60. – First consider $n = 8$. Again put $m = M_{\rho'\rho}$. Then as in equation (5.1) we get

$$0 \leq s_L^{(1,\,2)} = \frac{2}{\sqrt{3}\,n}\,(1 - m). \tag{6.1a}$$

Therefore either $m = 0$ or $m = 1$ (*i.e.* $\mathcal{K}_L^\rho = \{\,\rho\,\}$ or $\{\,\rho,\,\rho'\,\}$, respectively).

Next consider $n = 12$. Again put $m = \sum_{i=0}^{2} M_{A^i\rho,\,\rho}$ and $m' = \sum_{i=0}^{2} M_{A^i\rho',\,\rho}$. $m' = 0$ was done in Section 5, so consider here $m' > 0$.

Then as before, $m' \geq m$ and $m = 1$ or 3. Equation (5.2) becomes

$$0 \leq s_L^{(1,4)} = \frac{2}{\sqrt{3}\,n}\,(m - m')\left(\frac{\sqrt{3}}{2}\right). \tag{6.1b}$$

Therefore $m' = m = 1$ or 3. If $m = 3$ then $M_{\lambda\rho} = 0$ or 1 for all λ, by Lemma 1 (c), and $\mathcal{K}_L^\rho = \mathcal{O}_0\,\rho \cup \mathcal{O}_0\,\rho'$. But if $m = 1$, only one $\lambda \in \mathcal{O}_0\,\rho'$, say $\lambda = A^\ell\,\rho'$, has $M_{\lambda\rho} \neq 0$. Then we have $M_{A^i\rho',\,\rho} = \delta_{i\ell}$. To show this is impossible look now at $s_L^{(1,2)}$: depending on the value of ℓ this will either be non-real ($\ell = 1, 2$) or negative ($\ell = 0$).

Now consider the more difficult case $n = 24$. Write $\rho'' = (5, 5)$, $\rho''' = (7, 7)$, $m = \sum_{i=0}^{2} M_{A^i\rho,\,\rho}, \ldots, m''' = \sum_{i=0}^{2} M_{A^i\rho''',\,\rho}$. We may restrict ourselves to the case where $m'' > 0$ or $m''' > 0$, since $m'' = m''' = 0$ was done in Section 5. As usual, $m = 1$ or 3, and either $m' = 0$ or $m' \geq m$, and either $m'' = 0$ or $m'' \geq m$, and either $m''' = 0$ or $m''' \geq m$. Write $s\,(x)$ here for $\sin\,(\pi\,x/12)$. Then $s_L^{(2,2)}$, $s_L^{(3,3)}$ and $s_L^{(4,4)}$ give us

$$0 \leq 2\,(m - m' + m'' - m''')\,s\,(2) - (m - m' - m'' + m''')\,s\,(4), \tag{6.2a}$$

$$0 \leq 2\,(m + m' - m'' - m''')\,s\,(3) - (m - m' + m'' - m''')\,s\,(6), \tag{6.2b}$$

$$0 \leq 2\,(m - m' - m'' + m''')\,s\,(4) - (m - m' - m'' + m''')\,s\,(8), \tag{6.2c}$$

respectively. These give us

$$0 \leq m - m' - m'' + m''', \tag{6.3a}$$

$$0 \leq m - m' + m'' - m''', \tag{6.3b}$$

$$0 \leq m + m' - m'' - m''', \tag{6.3c}$$

In particular, equation (6.3*a*) comes immediatly from equation (6.2*c*); equation (6.3*b*) comes from equations (6.2*a*), (6.3*a*); and equation (6.3*c*) comes from equations (6.2*b*), (6.3*b*).

Now adding equations (6.3*a, b*), equations (6.3*a, c*), and equations (6.3*b, c*) give us $m' \leq m$, $m'' \leq m$, and $m''' \leq m$. So each m', m'', m''' will either equal 0 or m. If $m'' = m$, then equation (6.2*b*) tells us $m' = m''' = m$; if $m''' = m$, then equation (6.2*a*) tells us $m' = m'' = m$. Thus $m = m' = m'' = m''' = 1$ or 3.

As in the $n = 12$ case, $m = 3$ leads to the exceptional ρ-coupling given in Claim 7. If $m = 1$, there are numbers ℓ', ℓ'', ℓ''' such that $M_{A^i\,\rho',\,\rho} = \delta_{i\ell'}$,

$M_{A^i \rho'', \rho} = \delta_{i\ell''}$, and $M_{A^i \rho''', \rho} = \delta_{i\ell'''}$. This leads to 27 possibilities, all of which fail the $s_L^{(3,\,2)} \geq 0$ test.

Finally, consider $n = 60$. The reasoning and calculations are very similar to that for $n = 24$. Here, put $\rho'' = (11,\ 11)$, $\rho''' = (19,\ 19)$, and define $m,\ m',\ m'',\ m'''$ as before. Looking at $s_L^{(3,\,3)}$, $s_L^{(6,\,6)}$ and $s_L^{(10,\,10)}$ give us equations (6.3) again. As before, we can force $m = m' = m'' = m'''$ (use $s_L^{(3,\,3)}$ and $s_L^{(5,\,5)}$. But the difference here is that $s_L^{(2,\,5)} < 0$, so neither $m = 1$ nor $m = 3$ work. ■

Our next task is to handle the remaining case of Theorem 3: $n = 12$, so $f = (4,\ 4)$. First, on a computer we can find for each $\lambda = (a,\ b) \in \mathcal{P}_0$ all $\mu = (a',\ b') \in \mathcal{P}_0$ satisfying equation (2.1c) as well as the parity rule Lemma 4 (b). We find any $\lambda,\ \mu \in [(1,\ 1)] \cup [(5,\ 5)]$ satisfy these two conditions, as do any $\lambda,\ \mu \in [(2,\ 2)] \cup [(4,\ 4)]$, $\lambda,\ \mu \in [(3,\ 3)]$ and $\lambda,\ \mu \in [(1,\ 4)] \cup [(4,\ 1)]$. This means $M_{\lambda f} \neq 0$ only if $\lambda \in [(2,\ 2)] \cup [f]$, so we have to find $M_{(2,\,2),\,f}$, $M_{f,\,(2,\,2)}$ and $M_{f,\,f}$. If $M \neq \mathcal{D}_9, \mathcal{D}_9^c$, we must have $M_{(2,\,2),\,f} = M_{f,\,(2,\,2)} = 1$ (Lemma 3 (c) and a simple counting argument requires either both or neither of these values to be non-zero; equation (5.3) forces a non-zero value to be 1). Lemma 3 (b) says $M_{ff} \leq 3$, and only for $M_{ff} = 2$ does that block have the correct value for the Perron-Frobenius eigenvalue (namely, 3). Therefore $M_{ff} = 2$.

All we need to do is determine $\sigma\,[(5,\ 5)]$, $\sigma\,[(3,\ 3)]$, $\sigma\,[(1,\ 4)]$ and $\sigma\,[(1,\ 4)]$. Equation (2.1c) and the parity rule tell us $\sigma\,[(3,\ 3)] = [(3,\ 3)]$. That $\sigma\,[(5,\ 5)] = [(5,\ 5)]$ can be seen by Lemma 4 (a) with $\ell = 5$ applied to $M_{11,\,11}$. Now note that $M_{14,\,14} + M_{14,\,41} = 1$ (*i.e.* $\sigma\,[(1,\ 4)]$ equals either $[(1,\ 4)]$ or $[(4,\ 1)]$. Conjugating if necessary, we may assume $M_{14,\,14} = 1$. Then Lemma 4 (a) with $\ell = 5$ tells us $M_{41,\,41} = 1$. This determines all unknown matrix elements $M_{\lambda\mu}$, and we find we have $M = \mathcal{E}_9^{(2)}$.

Finally, we must address the exceptional couplings listed in Claim 7. Together, Theorems 1, 3 and 4 complete the $A_{2,\,k}$ classification, for any level k.

THEOREM 4. – (i) *For* $n = 8$, *if* $\mathcal{R} = \{\rho,\ \rho'\}$ *then* M *either equals* $\mathcal{E}_5$ *or its conjugation.*

(ii) *For* $n = 12$, *if* $\mathcal{R} = \mathcal{O}_0\,(1,\ 1) \cup \mathcal{O}_0\,(3,\ 3)$ *then* $M = \mathcal{E}_9^{(1)}$.

(iii) *For* $n = 24$, *if* $\mathcal{R} = \mathcal{O}_0\,(1,\ 1) \cup \mathcal{O}_0\,(5,\ 5) \cup \mathcal{O}_0\,(7,\ 7) \cup \mathcal{O}_0\,(11,\ 11)$ *then* $M = \mathcal{E}_{21}$.

Proof. – (i) We know from Claim 7 that $M_{\rho\lambda} = M_{\lambda\rho}$, for all λ, and that these all vanish except for $\lambda = (1,\ 1)$ and $\lambda = (3,\ 3)$, for which $M_{\rho\lambda} = M_{\lambda\rho} = 1$. Note that $(3\,\rho)^+ = (3,\ 3)$, and $(3\,(3,\ 3))^+ = \rho$. Therefore

Lemma 4 (a) with $\ell = 3$ applied to $M_{11,\,11} = 1$ gives us $M_{33,\,33} = 1$. Also, $M_{33,\,\mu} = M_{11,\,(3\mu)^+} = 0$ unless $\mu = \rho$ or (3, 3) (same for $M_{\lambda,\,33}$). Thus, if we expand M as in equation (2.4a), with $\rho \in \mathcal{I}(B_1)$ as usual, then $B_1 = B_{(1,\,2)}$ so Lemma 3 (b) tells us $r(B_i) = 2$ for all i, and each $M_{\lambda\mu} \leq 2$. We have reduced the number of possibilities for M to a finite number, and with a bit more effort can reduce this number further.

Lemma 1 (a) tells us that $\mathcal{P}_L = \mathcal{P}_R = [(1,1)] \cup [(3,3)] \cup [(1,3)] \cup [(3,1)]$. Again, equation (2.1$c$) and Lemma 4 ($b$) strongly restrict the possible couplings, and we find $M_{\lambda\mu} \neq 0$ only for $\lambda,\,\mu \in [(1,\,1)] \cup [(3,\,3)]$, or for $\lambda,\,\mu \in \mathcal{O}(1,\,3)$. The relation $S^{(n)}M = MS^{(n)}$ evaluated at ((6, 1), ρ) tells us that $M_{61,\,16} + M_{61,\,61} = M_{61,\,32} + M_{61,\,23} = 1$; without loss of generality (by conjugating if necessary) we may suppose $M_{61,\,61} = 1$. Then equation (2.3e) tells us $t(\lambda) \equiv_3 t(\mu)$ whenever $M_{\lambda\mu} \neq 0$, as well as $M_{A\lambda,\,A\mu} = M_{\lambda\mu}$.

M is now fixed once we determine whether $M_{13,\,13} = 0, 1, 2$. But $M_{13,\,13} = 1$ is fixed by $(S^{(8)}M)_{13,\,12} = (MS^{(8)})_{13,\,12}$.

(ii) This is easier. Lemma 1 (a) says $\mathcal{P}_L = \mathcal{P}_R = [(1,\,1)] \cup [(3,\,3)] \cup [(5,\,5)]$. Equation (2.1$c$) and Lemma 4 ($b$) tell us $M_{\lambda\mu} \neq 0$ implies λ, $\mu \in [(1,\,1)] \cup [(5,\,5)]$ or $\lambda,\,\mu \in [(3,\,3)]$. $\mathcal{J}_L = \mathcal{J}_R = \mathcal{O}_0$, so Lemma 1 ($c$) tells us the only independent parameters are $M_{11,\,11} = M_{11,\,55} = M_{55,\,11} = 1$, $M_{55,\,55}$ and $M_{33,\,33}$. $M_{55,\,55} = 1$ by Lemma 4 (a) using $\ell = 5$ and $M_{11,\,11} = 1$, so (using usual notation) $B_1 = B_{(1,\,6)}$. But $B_2 = B_{(M_{33,\,33},\,3)}$ so $3\,M_{33,\,33} = r(B_2) = r(B_1) = 6$, *i.e.* $M_{33,\,33} = 2$. We have derived $M = \mathcal{E}_9^{(1)}$.

(iii) $\mathcal{P}_L = \mathcal{P}_R = [(1,\,1)] \cup [(5,\,5)] \cup [(7,\,7)] \cup [(11,\,11)] \cup [(5,\,8)] \cup [(8,\,5)] \cup [(1,\,7)] \cup [(7,\,1)]$. Equation (2.1$c$) tells us $M_{\lambda\mu} \neq 0$ implies either $\lambda,\,\mu \in [(1,\,1)] \cup [(5,\,5)] \cup [(7,\,7)] \cup [(11,\,11)]$ or $\lambda,\,\mu \in [(5,\,8)] \cup [(8,\,5)] \cup [(1,\,7)] \cup [(7,\,1)]$. Lemma 4 ($a$) applied to $\ell = 5, 7, 11$ and to $M_{11,\,11} = M_{11,\,55} = M_{11,77} = M_{11,\,1111} = 1$ tells us $M_{aa,\,bb} = 1$ for each choice $a,\,b = 1, 5, 7, 11$. Also, $\mathcal{J}_L = \mathcal{J}_R = \mathcal{O}_0$. Together with Lemma 1 (c), we find that $B_1 = B_{1,\,12}$.

Note that from Lemmas 4 (a) and 1 (c), we can similarly deduce all the remaining values of $M_{\lambda\mu}$ once we known the four values $M_{58,\,58}$, $M_{58,\,85}$, $M_{58,\,17}$, $M_{58,\,71}$. In fact we find from Lemmas 4 (a) and 1 (c) that for each $\lambda \in [(5,\,8)] \cup [(8,\,5)] \cup [(1,\,7)] \cup [(7,\,1)]$, each row sum $\sum_\mu M_{\lambda\mu}$ is equal (*i.e.* independent of λ). Equation (2.4b) then tells us these sums must equal $r(B_1) = 12$, so $M_{58,\,58} + M_{58,\,85} + M_{58,\,17} + M_{58,\,71} = 4$. Now, evaluating $S^{(n)}M = MS^{(n)}$ at (58, ρ), (58, 14) and (58, 25), we obtain $M_{58,\,58} = M_{58,\,85} = M_{58,\,17} = M_{58,\,71} = 1$, so $M = \mathcal{E}_{21}$. ■

7. CONCLUDING REMARKS

In this paper we rewrote the classification in [1], paying attention to the points mentioned in the abstract.

There still are few completed modular invariant classifications. *See* ref. [1] for the references to the older results: $g = A_1$, $\forall\, k$; g simple, $k = 1$; $c = 1$ RCFTs; parafermions, etc. Some of the new classifications are the *simple-current invariants* [22]. Among other things, [17] completes the classification for $A_{1,\,k_1} \oplus A_{1,\,k_2}$, $\forall\, k_1$, k_2. All heterotic invariants of small rank are now known [23], as are most (all?) of the $c = 24$ meromorphic theories [24]. Classifications have recently been found [13] for diagonal GKO cosets at certain levels corresponding to A_1 and A_2. Most physical invariants turn out to be "obvious" – *i.e.* either due to outer automorphisms of the affine algebra, or to conformal embeddings, in the standard ways. But new exceptionals are always being found (most recently, in [27]). Indeed, a somewhat convincing argument [24] for the practical impossibility of a classification of all physical invariants for all (semi-simple) g is the large number of exceptionals; however simple g is much better behaved in this regard.

This paper has been written with the classification for all affine $g^{(1)}$ in mind. In particular, the following 3-step approach is suggested by the proof in this paper:

Step 1) find all automorphism invariants;

Step 2) find all automorphisms of simple current extensions;

Step 3) find all exceptional extensions and their automorphisms.

Step 1 is now complete ([25], [26]) for all g simple, as well as $g = A_{n_1} \oplus \cdots \oplus A_{n_s}$. The proof is a natural generalization of the one given in Section 3 of this paper. The argument given in Section 5 of this paper makes it clear that Step 2 should also be possible for all g; indeed this has recently been done for all $g = A_n$ [29]. Step 3 would then be the remaining barrier for the classification of all WZW partition functions. Here it was accomplished using the parity rule. The question is not the power of the parity rule – it appears to remain potent at arbitrary rank and level – but rather the difficulty in applying it. However the S matrix is extremely interesting mathematically and there can be little doubt that other of its many properties will also prove useful.

Future work along these lines include attempting to find all automorphism invariants for all semi-simple g (this would complete the classification of all WZW CFTs whose maximally extended chiral algebra is an affine algebra), and finding all possible automorphism invariants for the simple-current extensions of theories with simple $g \neq A_n$. The former should follow from the arguments in ([25], [26]), while the latter should follow from the arguments of [29]. Step 3 will not be generalizable to arbitrary g until Section 4 of this paper is considerably simplified. There are many ways to imagine doing this, among them the following: using the Knizhnik-Zamolodlchikov equation approach of [11]; using various number fields [6]; assigning the level and rank a more " dynamic" role to play in the arguments, e.g. by taking large k limits; exploiting more of the algebraic structure of the commutant.

But isolated classifications can be rather sterile. The interesting thing is to see if they shed any new light on the subject, e.g. disclose new connections or possibilities involving other areas of math or physics. Indeed this seems to be the case with these modular invariant classifications. The most famous example is the A-D-E classification of the $A_{1,k}$ physical invariants [28]. This $A_{2,k}$ classification also hints of deep interconnections with other areas. Indeed [8] has discovered a fascinating connection involving Fermat curves [10]. The names assigned to the physical invariants in equations (1.7) were given by analogy with the A-D-E classification, but it would be interesting and important to understand what form A-D-E actually takes in our SU(3) list. For this author personally, trying to understand a little better these deep mysteries is the main motivation to continue working in this area.

There are many interconnections between modular invariants of different algebras and levels. One example is rank-level duality: e.g. it is easy to see that the parity rule for $A_{\ell,k}$ is isomorphic to that of $A_{k-1,\ell+1}$. Other examples can be seen in this paper. For example when $n \equiv_4 0$, the parity rule $\varepsilon(\ell\lambda) = \varepsilon(\ell\mu)$, $\ell \in C_n$, for $A_{2,n-3}$ is intimately connected with that for $A_{1,n/2-2}$ and $A_{2,n/2-3}$ – exactly how depends on the values of λ_1, λ_2, μ_1, μ_2 (mod 2). We saw the $\mu = \rho$ case of this in the proof of Proposition 1. The "reason" for these connections is that $\ell \in C_n$ iff $\ell + n/2 \in C_n$ for these n. It is natural to try to better understand and exploit these various interconnections.

ACKNOWLEDGEMENTS

A number of people supported me at various stages of [1], as well as this paper. I would particularly like to thank Patrick Roberts, who was my sounding board through this whole process. I also benefitted throughout from conservations with Quang Ho-Kim and C. S. Lam, and more recently with Antoine Coste, Krzysztof Gawedzki, Claude Itzykson, Jean Lascoux, Philippe Ruelle, Yassen Stanev, Mark Walton, and Jean-Bernard Zuber. The generosity of the IHES is also greatly appreciated.

REFERENCES

[1] T. GANNON, The classification of affine SU(3) modular invariant partition functions, *Commun. Math. Phys.*, Vol. **161**, 1994, pp. 233-264.

[2] G. MOORE and N. SEIBERG, Naturality in conformal field theory, *Nucl. Phys.*, Vol. **B313**, 1989, pp. 16-40.

[3] V. G. KAC, Infinite Dimensional Lie Algebras, 3rd ed., Cambridge University Press, Cambridge, 1990.

[4] V. G. KAC and D. PETERSON, Infinite-dimensional Lie algebras, theta functions and modular forms, *Adv. Math.*, Vol. **53**, 1984, pp. 125-264.

[5] M. BAUER and C. ITZYKSON, Modular transformations of SU(N) affine characters and their commutant, *Commun. Math. Phys.*, Vol. **127**, 1990, pp. 617-636.

[6] Ph. RUELLE, E. THIRAN and J. WEYERS, Modular invariants for affine Su(3) theories at prime heights, *Comm. Math. Phys.*, Vol. **133**, 1990, pp. 305-322.

[7] T. GANNON, WZW commutants, lattices, and level-one partition functions, *Nucl. Phys.*, Vol. **B396**, 1993, pp. 708-736.

[8] Ph. RUELLE, E. THIRAN and J. WEYERS, Implications of an arithmetical symmetry of the commutant for modular invariants, *Nucl. Phys.*, Vol. **B402**, 1993, pp. 693-708.

[9] Ph. RUELLE, Automorphisms of the affine SU(3) fusion rules, *Commun. Math. Phys.*, Vol. **160**, 1994, pp. 475-492.

[10] N. KOBLITZ and D. ROHRLICH, Simple factors in the Jacobian of a Fermat curve, *Can. J. Math.*, Vol. **XXX**, 1978, pp. 1183-1205.

[11] Y. STANEV, Classification of the local extensions of the SU(3) chiral current algebra, Vienna preprint ESI-19, 1993.

[12] L. BÉGIN, P. MATHIEU and M. WALTON, $\widehat{su}(3)_k$ fusion coefficients, *Mod. Phys. Lett.*, Vol. **A7**, 1992, pp. 3255-3265.

[13] T. GANNON and M. A. WALTON, On the classification of diagonal coset modular invariants, *Commun. Math. Phys.*, Vol. **173**, 1995, pp. 175-198.

[14] D. ALTSCHULER J. LACKI and Ph. ZAUGG, The affine Weyl group and modular invariant partition functions, *Phys. Lett.*, Vol. **B205**, 1988, pp. 281-284.

[15] D. BERNARD, String characters from Kac-Moody automorphisms, *Nucl. Phys.*, Vol. **B288**, 1987, pp. 628-648.

[16] P. CHRISTE and F. RAVANANI, $G_N \otimes G_{N+L}$ conformal field theories and their modular invariant partition functions, *Int. J. Mod. Phys.*, Vol. **A4**, 1989, pp. 897-920.

[17] T. GANNON, Towards a classification of $\mathrm{SU}(2) \oplus \cdots \oplus \mathrm{SU}(2)$ modular invariant partition functions, *J. Math. Phys.*, Vol. **36**, 1995, pp. 675-706.

[18] F. R. GANTMACHER, The theory of matrices, Vol. II, Chesea Publishing Co., New York, 1964.

[19] A. COSTE and T. GANNON, Remarks on Galois symmetry in RCFT, *Phys. Lett.*, Vol. **B323**, 1994, pp. 316-321.

[20] N. BOURBAKI, Groupes et Algèbres de Lie, Chapitre IV-VI, Hermann, Paris, 1968.

[21] T. GANNON and Q. HO-KIM, The low level modular invariant partition functions or rank 2 algebras, *Int. J. Mod. Phys.*, Vol. **A9**, 1994, pp. 2667-2686.

[22] M. KREUZER and A. N. SCHELLEKENS, Simple currents versus orbifolds with discrete torsion – a complete classification, *Nucl. Phys.*, Vol. **B411**, 1994, pp. 97-121.

[23] T. GANNON and Q. HO-KIM, The rank-four heterotic modular invariant partition functions, *Nucl. Phys.*, Vol. **B425**, 1994, pp. 319-342.

[24] A. N. SCHELLEKENS, Meromorphic $c = 24$ conformal field theories, *Commun. Math. Phys.*, Vol. **153**, 1993, pp. 159-185; P. MONTAGUE, Orbifold construction and the classification of self-dual $c = 24$ conformal field theories, (hep-th/9403088).

[25] T. GANNON, Symmetries of Kac-Peterson modular matrices of affine algebras, *Invent. Math.*, Vol. **122**, 1995, pp. 341-357.

[26] T. GANNON, Ph. RUELLE and M. A. WALTON, Automorphism modular invariants of current algebras, (hep-th/9503141).

[27] J. FUCHS, A. N. SCHELLEKENS and C. SCHWEIGERT, Galois modular invariants of WZW models, *Nucl. Phys.*, Vol. **B437**, 1995, pp. 667.

[28] A. CAPPELLI, C. ITZYKSON and J.-B. ZUBER, The A-D-E classification of $A_1^{(1)}$ and minimal conformal field theories, *Commun. Math. Phys.*, Vol. **113**, 1987, pp. 1-26.

[29] T. GANNON, Kac-Peterson, Perron-Frobenius, and the Classification of Conformal Field Theories (q-alg/9510026).

(Manuscript received December 1, 1994;
Revised version received July 3, 1995.)