On parity functions in conformal field theories

1999 J. Phys. A: Math. Gen. 32 3555

(http://iopscience.iop.org/0305-4470/32/19/307)

J. Phys. A: Math. Gen. **32** (1999) 3555–3570. Printed in the UK PII: S0305-4470(99)97718-1

On parity functions in conformal field theories

D Altschüler†, P Ruelle‡§ and E Thiran‡

† Département de Mathématiques, Université de Nantes, BP 92208, F-44322 Nantes Cedex 03, France

‡ Institut de Physique Théorique, Université Catholique de Louvain, B-1348 Louvain-La-Neuve, Belgium

Received 18 September 1998, in final form 4 February 1999

Abstract. We examine general aspects of parity functions arising in rational conformal field theories, as a result of Galois theoretic properties of modular transformations. We focus more specifically on parity functions associated with affine Lie algebras, for which we give two efficient formulae. We investigate the importance of these for the modular invariance problem.

1. Introduction

Modular invariance has become a major tool in the ambitious programme of classifying all rational conformal field theories (RCFTs). At genus one, modular invariance is the requirement that a RCFT can be put on a torus in a consistent way, so that, for example, the partition function should be well defined over the conformal classes of tori [1]. Since the seminal ADE classification of the Wess–Zumino–Novikov–Witten (WZNW) models based on $su(2)$ [2], there has been much progress on this question, especially during the last few years, which have seen arithmetical techniques come into play. In particular, the technical analysis of the conditions expressing the modular invariance of the partition function on the torus has shown that the use of Galois theory leads to powerful restrictions. These restrictions are now usually referred to as parity selection rules. They have had a crucial role in various classification results, that of the $su(3)$-based WZNW being amongst the most convincing [3].

This paper is devoted to the study of general properties of the parity selection rules corresponding to the best known RCFTs, namely the WZNW models. We will be more general and consider theories with symmetry algebras given by isomorphic chiral affine Lie algebras.

After reviewing the basics of the modular invariance problem and the technical questions associated with it in the case of affine Lie algebras, we present in section 3 two new explicit formulae for the parities which serve us as starting points for the results that follow. The first of these expresses the parities in a given algebra as products of parities in the simplest one, namely $su(2)$. For obvious reasons, we call it a multiplicative formula. The second formula, which we call additive, is perhaps more surprising, as it allows us to compute the affine parities through modular arithmetics on the Dynkin labels of weights. In terms of computational efficiency, these formulae are easier to use than the existing ones. We elaborate on them in the last two sections.

§ Chercheur Qualifié FNRS.

0305-4470/99/193555+16$19.50

In section 4, we consider the multiplicative formula, and show that the parity selection rules amount to check whether the product of two specific S-matrix elements, namely $S_{0,i}S_{0,j}$, is totally positive (see section 4 for a definition). Relying on this, we then proceed to construct solutions to the selection rules via the use of trigonometric (cyclotomic) identities. We argue that these solutions are generic albeit not exhaustive. For reasons explained there, their use for the modular invariance problem remains difficult.

We explore in section 5 the consequences of the second, additive formula. We show that the parity selection rules can be turned into algebraic equations in a finite ring. This approach comes close to deeper arithmetical quantities like the generalized Bernoulli numbers, but appears to point to deep arithmetical problems. However, in our opinion, this path looks more promising despite the technical obstacles. A reason for this is that the problem can be divided into two parts. One is entirely concerned with arithmetical questions (related to number theoretic properties of cyclotomic extensions), while the other depends on which specific algebra is being treated. Since the first part seems to be the more difficult, we hope that this approach could lead to the solution of the parity selection rules for more than one affine algebra.

As the parity functions are naturally cohomological objects, the appendix collects certain results concerning the cohomology that is appropriate to them. Among other things, we prove identities relating the parity functions pertaining to different affine Lie algebras (mainly $su(2N+1)$ parities with $su(2N)$ parities).

2. Preliminaries and notation

We first fix the notation regarding affine Lie algebras (referring to [4] for further details) and recall their modular properties. We denote by $\mathcal{G}$ a finite simple Lie algebra. The untwisted level k affine algebra $\widehat{\mathcal{G}}_k$ based on $\mathcal{G}$ is generated by $\mathcal{G}$-valued currents $J(z)$ satisfying the following commutation rules

$$[\langle T^a, J(z)\rangle, \langle T^b, J(w)\rangle] = \langle [T^a, T^b], J(z)\rangle \delta(z-w) + k\langle T^a, T^b\rangle \partial_z \delta(z-w) \tag{2.1}$$

where $\{T^a\}$ is a set of generators for $\mathcal{G}$. When $k \geqslant 0$ is an integer, the algebra $\widehat{\mathcal{G}}_k$ has a finite number of unitary irreducible representations $L(p)$, labelled by the strictly dominant weights of $\mathcal{G}$ in the alcove $P^n_{++}(\mathcal{G})$

$$P^n_{++}(\mathcal{G}) = \left\{ p = (a_1, a_2, \ldots) : a_i > 0, \text{ and } \sum_i k_i^\vee a_i < n \right\} \tag{2.2}$$

where $k_i^\vee$ are the Kac labels given by the decomposition of the highest root into simple roots $\psi = \sum_i k_i^\vee \alpha_i$ and where we have set $n = k + h^\vee$ with $h^\vee = \varrho \cdot \psi + 1$ the dual Coxeter number of $\mathcal{G}$ and ϱ is half the sum of the positive roots. The normalization of the scalar product is such that $\psi^2 = 2$. In the following we will almost exclusively use the integer n, called the height, instead of k. We let $\chi_p(\tau)$ be the specialized character of $L(p)$.

The alcove P^n_{++} is an affine Weyl chamber, that is, it is the quotient of the weight lattice of $\mathcal{G}$ minus the union of all affine walls by the action of the affine Weyl group $\widehat{W}_n(\mathcal{G})$ of height n. Since the affine Weyl transformations $\hat{w}$ have well defined parity, one can associate to any weight p a number $\varepsilon_n(\mathcal{G}; p)$ as follows

$$\varepsilon_n(\mathcal{G}; p) = \begin{cases} 0 & \text{if } p \text{ is in an affine wall} \\ +1 & \text{if } \hat{w}(p) \in P^n_{++} \text{ for an even } \hat{w} \\ -1 & \text{if } \hat{w}(p) \in P^n_{++} \text{ for an odd } \hat{w}. \end{cases} \tag{2.3}$$

For obvious reasons, $\varepsilon_n(\mathcal{G}; p)$ will be called the affine parity of p (relative to $\widehat{W}_n(\mathcal{G})$). It is well defined on the weight lattice on account of the fact that $\widehat{W}_n(\mathcal{G})$ fixes the set of affine walls, and has a free action elsewhere. It satisfies the following properties

$$\begin{aligned}&\varepsilon_n(\mathcal{G}; \hat{w}(p)) = (\det \hat{w})\, \varepsilon_n(\mathcal{G}; p)\\ &\varepsilon_n(\mathcal{G}; p + n\alpha^\vee) = \varepsilon_n(\mathcal{G}; p) \qquad \text{for any co-root } \alpha^\vee.\end{aligned} \tag{2.4}$$

The Hilbert space of a conformal theory with symmetry algebra $\widehat{\mathcal{G}}_k \times \widehat{\mathcal{G}}_k$ consists of representations $L(p) \otimes L(p')$ taken with certain multiplicities $N_{p,p'}$

$$\mathcal{H} = \bigoplus_{p,p'} N_{p,p'}(L(p) \otimes L(p')) \qquad N_{p,p'} \in \mathbb{N}. \tag{2.5}$$

When the theory is put on a torus of modulus τ, the partition function takes the form [1]

$$Z(\tau, \tau^*) = \sum_{p,p'} N_{p,p'} \chi_p(\tau) \chi^*_{p'}(\tau). \tag{2.6}$$

Since two tori with moduli τ and $(a\tau + b)/(c\tau + d)$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in PSL(2, \mathbb{Z})$, are conformally equivalent, a consistency condition is that the partition function must be modular invariant, that is, $Z(\tau) = Z((a\tau + b)/(c\tau + d))$. The modular group $PSL(2, \mathbb{Z})$ is generated by $\tau \to \tau + 1$ and $\tau \to -1/\tau$, it is sufficient to check the invariance of $Z(\tau)$ under these two substitutions.

For affine Lie algebras, it is known that the characters carry a linear representation of the modular group [4] (the same is true of all known RCFTs, although no general proof exists). Explicitly, one has

$$\chi_p(\tau + 1) = \sum_{p'} T_{p,p'} \chi_{p'}(\tau) \qquad \chi_p(-1/\tau) = \sum_{p'} S_{p,p'} \chi_{p'}(\tau) \tag{2.7}$$

with T and S both symmetric and unitary. T is diagonal with roots of unity on the diagonal, while S is more complicated. The crucial property for what follows is that S, like T, has all its entries in a cyclotomic extension of the rationals (if one assumes the existence of unitary matrices S and T, this is in fact true in any RCFT, as proved in [5]). This implies that the algebraic extension $\mathbb{M} \equiv \mathbb{Q}(S_{p,p'})$ generated by the coefficients of S is a Galois extension with Abelian Galois group. $\mathbb{M}$ contains the subfield $\mathbb{L} \equiv \mathbb{Q}(S_{p,p'}/S_{p,\varrho})$, of which $\mathbb{M}$ is at most a quadratic extension (by $S_{\varrho,\varrho}$). The action on S of the Galois group of $\mathbb{M}$ is particularly simple. Take $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$. It has been shown [5] that σ induces a permutation of the weights in P^n_{++}, such that

$$\sigma(S_{p,p'}) = \varepsilon_\sigma(p) S_{\sigma(p),p'} = \varepsilon_\sigma(p') S_{p,\sigma(p')} \qquad \varepsilon_\sigma(p) \in \{\pm 1\}. \tag{2.8}$$

Because $S^2_{p,p'} \in \mathbb{L}$, the permutation of P^n_{++} induced by σ is determined only through its restriction to $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. The numbers $\varepsilon_\sigma(p)$, called Galois parities, are not representations of the Galois group, but rather co-cycles, satisfying $\varepsilon_{\sigma\sigma'}(p) = \varepsilon_\sigma(\sigma'(p))\varepsilon_{\sigma'}(p)$. They are the central objects of this paper. In a general RCFT, the relations (2.8) are still valid if we take p and p' as labels for the set $\mathcal{P}$ of primary fields.

If one inserts the modular transformations of the characters in the partition function (2.6), requiring its modular invariance, one obtains the condition that the matrix N must commute with T and S (one assumes also that the characters can be fully disentangled by additional Cartan variables or by a discrete charge). Then by acting with an element σ of the Galois group of $\mathbb{M}$ on the equation $[N, S] = 0$, one obtains the important result that

$$N_{\sigma(p),\sigma(p')} = \varepsilon_\sigma(p)\varepsilon_\sigma(p') N_{p,p'}. \tag{2.9}$$

The parity selection rules now follow from the requirement that the coefficients of N must be positive integers

$$\varepsilon_\sigma(p)\varepsilon_\sigma(p') = -1 \text{ for some } \sigma \text{ in } \mathrm{Gal}(\mathbb{M}/\mathbb{Q}) \quad \Longrightarrow \quad N_{p,p'} = 0. \tag{2.10}$$

On the other hand, if $\varepsilon_\sigma(p)\varepsilon_\sigma(p') = +1$ for all σ, then $N_{p,p'}$ can be non-zero, in which case we say that there is a coupling between p and p'.

Therefore, in order to know which $N_{p,p'}$ can be non-zero and which are to vanish, it is of paramount importance to solve the parity equation, i.e. to know all pairs of weights (p, p') that satisfy

$$\varepsilon_\sigma(p) = \varepsilon_\sigma(p') \qquad \text{for all } \sigma. \tag{2.11}$$

This equation is the key ingredient to most classification results, but is notoriously hard to solve.

These selection rules hold in any RCFT in which the characters transform in a unitary representation of the modular group. They put very strong restrictions on the multiplicities of the representations (of whichever algebra is present) that build the Hilbert space and thus on the field content of the theory. Note that they have a purely group theoretical origin, as the parity functions are completely determined once the chiral algebras hence the characters are chosen. In case the left and right chiral algebras are not isomorphic, restrictions like (2.10) apply, if appropriate parity functions are used. We end this introductory section by making these functions explicit for affine Lie algebras.

In the case of affine Lie algebras, it is known that S is equal to [4]

$$S_{p,p'} = \gamma(\mathcal{G}, n) \sum_{w\in W(\mathcal{G})} (\det w)\, \mathrm{e}^{-2\mathrm{i}\pi p\cdot w(p')/n}. \tag{2.12}$$

with W the finite Weyl group and $\gamma(\mathcal{G}, n)$ a numerical constant. The numbers $S_{p,p'}$ belong to the cyclotomic extension $\mathbb{Q}(\zeta_{nQ})$—ζ_m will denote a primitive mth root of unity—for some integer Q depending on $\mathcal{G}$ (and possibly on n, see [9, 10]). The elements of $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ are indexed by integers h co-prime with nQ, i.e. by elements of $\mathbb{Z}^*_{nQ}$. The Euler function $\varphi(nQ)$ gives the order of $\mathbb{Z}^*_{nQ}$.

From the formula for $S_{p,p'}$, it is not difficult to compute the permutation of the alcove induced by σ_h: $\sigma_h(p)$ is the only weight in the alcove whose image by an affine Weyl transformation is the dilated weight hp (multiplication component-wise). In other words, there exists a unique $w_{h,p} \in W(\mathcal{G})$ and a unique co-root $\alpha^\vee_{h,p}$ of $\mathcal{G}$ such that $\sigma_h(p) = w_{h,p}(hp)+n\alpha^\vee_{h,p}$. Moreover, the Galois parity becomes

$$\varepsilon_{\sigma_h}(p) = \frac{\sigma_h(\gamma(\mathcal{G}, n))}{\gamma(\mathcal{G}, n)}\varepsilon_n(\mathcal{G}; hp) \tag{2.13}$$

which is an affine parity up to a constant prefactor (itself a sign because $[\gamma(\mathcal{G}, n)]^2 \in \mathbb{Q}$). Since this prefactor does not depend on p, it clearly drops out of the selection rules (2.10)—it would, however, matter if the chiral algebras were not isomorphic—so we neglect it from now on (except in the appendix). Therefore, the parity equation for affine Lie algebras takes the form

$$\varepsilon_n(\mathcal{G}; hp) = \varepsilon_n(\mathcal{G}; hp') \qquad \forall h \in \mathbb{Z}^*_{nQ}. \tag{2.14}$$

Note that the map $h \longmapsto \sigma_h(\gamma(\mathcal{G}, n))/\gamma(\mathcal{G}, n) = \pm 1$ is an homomorphism, so that the affine parity $\varepsilon_n(\mathcal{G}; hp)$ itself is a co-cycle.

An algorithm to compute the parity of an arbitrary weight can be given, that requires evaluating congruences on Dynkin labels and determinants of permutations (see [6] for $\mathcal{G} = A_\ell$). It is not our purpose to describe that algorithm in the general case, since, as we shall soon see, $\mathcal{G}$ parities can be reduced to the much simpler $su(2)$ parities, which we now make explicit.

In the Dynkin basis, an $su(2)$ weight is just an integer and the weight lattice is $\mathbb{Z}$. The dual Coxeter number is $h^\vee = 2$ so that the alcove at height n is the set

$$P^n_{++}(su(2)) = \{a \in \mathbb{Z} : 1 \leqslant a \leqslant n - 1\}. \tag{2.15}$$

The affine walls are the points of the ideal $n\mathbb{Z}$. The co-roots correspond to even integers, which implies that the parity function of $su(2)$ is periodic with period $2n$. Therefore, it only depends on the residue modulo $2n$ of its argument, which we denote by $\langle a\rangle_{2n}$, taken between 0 and $2n-1$. (More generally, we denote by $\langle x\rangle_y$ the residue of x modulo y, chosen in $[0, y-1]$.) Putting this together, we find for any integer a

$$\varepsilon_n(a) \equiv \varepsilon_n(su(2); a) = \begin{cases} 0 & \text{if } a = 0 \bmod n \\ +1 & \text{if } \langle a\rangle_{2n} < n \\ -1 & \text{if } \langle a\rangle_{2n} > n. \end{cases} \tag{2.16}$$

This is confirmed by computing directly the action of the Galois group on the S matrix, given for $su(2)$ by $S_{a,a'} = (2/n)^{1/2}\sin(\pi aa'/n)$. For later use, we collect the main properties of the $su(2)$ parity

$$\varepsilon_n(a) = \operatorname{sgn}\left(\sin\frac{\pi a}{n}\right) = 2 - \frac{\langle a\rangle_{2n} + \langle n-a\rangle_{2n}}{n} \qquad a \notin n\mathbb{Z} \tag{2.17}$$

$$\varepsilon_n(a) = \varepsilon_n(n-a) = \varepsilon_n(a+2n) = -\varepsilon_n(-a). \tag{2.18}$$

To summarize, the main conclusion, as far as affine Lie algebras are concerned, is that Galois parities coincide with affine parities. Solving the parity equation (2.14) is nonetheless extremely hard, which explains why the general solution is known for $su(2)$† and $su(3)$ only. For $su(2)$, the result is fairly simple, even though the proof is not completely straightforward, despite the deceptive simplicity of the parity function. In the case of $su(3)$, the parity equation is considerably more complex and it is only recently that the general solution has been given [7], though in a totally different context. As noticed in [6], the $su(3)$ parity plays a fundamental role in the description of the Jacobian varieties of the complex Fermat curves and it is in this geometric setting that, in disguise, the equation for $su(3)$ was solved in all generality (see [8] for a review of the connections between the two problems). The $su(3)$ solution yields, as a special case, the solution for the $su(2)$ case. For higher rank algebras, virtually nothing is known about the parity equation.

It is our purpose here to suggest new directions, by showing that some of the properties that proved very useful for the $su(2)$ and $su(3)$ algebras, in fact go over to other cases.

One may also note that focusing on $su(2)$ parities is not only important for dealing with parities arising in affine algebras, they turn out to be relevant in other models as well. Good examples are provided by minimal conformal theories $\mathcal{M}(p, q)$, in which the Galois parities are just products of two $su(2)$ parities, taken at heights p and q. Because the S matrices in rational conformal theories are often related to sine functions, $su(2)$ parities inevitably emerge when acting with the Galois groups. This should be no surprise as most known rational theories can be constructed as cosets of WZNW models.

3. Formulae for parities

We will present in this section two explicit formulae to compute the parity functions in affine algebras. They have very different qualities, one being multiplicative, the other additive. Perspectives offered by these formulae are investigated in subsequent sections.

The first, multiplicative, formula relates the parity in any (untwisted) affine algebra to the parity function in the simplest of all, namely $su(2)$. For p a weight of $\mathcal{G}$, not necessarily

† At the time the classification of affine $su(2)$ modular invariant partition functions was completed [2], the Galois symmetry of the S matrix had not yet been recognized and consequently there was no parity equation. The now available general solution of the $su(2)$ parity equation would yield the result in a more efficient way.

dominant, the following formula yields an expression for the parity of p relative to the affine Weyl group $\widehat{W}_n(\mathcal{G})$

$$\varepsilon_n(\mathcal{G};\, p) = \prod_{\text{roots } \alpha>0} \varepsilon_{nD}(su(2);\, D\alpha\cdot p) = \prod_{\alpha>0} \operatorname{sgn}\left(\sin\frac{\pi\alpha\cdot p}{n}\right) \tag{3.1}$$

where D is the smallest positive integer such that $D\alpha\cdot p \in \mathbb{Z}$ for all weights p and all roots α. Explicitly $D = 1$ for $\mathcal{G}$ simply-laced, $D = 2$ for $\mathcal{G} = B_\ell, C_\ell, F_4$ and $D = 3$ for $\mathcal{G} = G_2$.

The proof of the product formula (3.1) is not difficult. One may first check that both expressions coincide when p is in the fundamental alcove $P^n_{++}(\mathcal{G})$ (clear because p in the alcove implies $\alpha\cdot p \in [1, n-1]$), and then verify that they have the same transformation properties under the affine Weyl group. For the translational part, one uses, for any co-root $\alpha^\vee$

$$\frac{\varepsilon_n(\mathcal{G};\, p + n\alpha^\vee)}{\varepsilon_n(\mathcal{G};\, p)} = \prod_{\alpha>0} \frac{\varepsilon_{nD}(D\alpha\cdot p + nD\alpha\cdot\alpha^\vee)}{\varepsilon_{nD}(D\alpha\cdot p)} = \prod_{\alpha>0}(-1)^{\alpha\cdot\alpha^\vee} = (-1)^{2\varrho\cdot\alpha^\vee} = +1. \tag{3.2}$$

For the finite Weyl part, one checks

$$\begin{aligned}\prod_{\alpha>0} \varepsilon_{nD}(D\alpha\cdot w(p)) &= \prod_{\alpha>0} \varepsilon_{nD}(Dw^{-1}(\alpha)\cdot p)\\ &= (-1)^{t_w} \prod_{\alpha>0} \varepsilon_{nD}(D\alpha\cdot p) = (\det w) \prod_{\alpha>0} \varepsilon_{nD}(D\alpha\cdot p)\end{aligned} \tag{3.3}$$

with t_w the number of positive roots whose image under w are negative roots.

Alternatively one may obtain the formula (3.1) by acting with an element of the Galois group $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ on the factorized form for the S matrix elements

$$S_{\varrho,p}(\mathcal{G}) = \gamma'(\mathcal{G}, n) \prod_{\alpha>0} S_{\varrho,\alpha\cdot p}(su(2)) \tag{3.4}$$

for some constant γ' that only depends on $\mathcal{G}$ and n.

Our second formula is additive and has a stronger arithmetical character. According to the previous, multiplicative expression, parity functions in affine algebras are products of $su(2)$ parities $\varepsilon_n(\alpha\cdot p)$ (say when $D = 1$). As mentioned before, these $su(2)$ parities depend on the residues of their argument modulo $2n$. However, in the particular case $\mathcal{G} = su(3)$, the parity function, a product of three $su(2)$ parities according to (3.1)

$$\varepsilon_n(su(3);\, p) = \varepsilon_n(a)\varepsilon_n(b)\varepsilon_n(a+b) = \varepsilon_n(a)\varepsilon_n(b)\varepsilon_n(n-a-b) \qquad p = (a, b) \tag{3.5}$$

can also be written in a way that only involves residues modulo n. Indeed one may check that

$$\varepsilon_n(su(3);\, p) = \begin{Bmatrix} +1 \\ -1 \end{Bmatrix} \quad\Longleftrightarrow\quad \langle a\rangle_n + \langle b\rangle_n + \langle n-a-b\rangle_n = \begin{Bmatrix} n \\ 2n \end{Bmatrix}. \tag{3.6}$$

Since this additive formula proved extremely useful to solve the parity equation for $su(3)$ [7, 11], it is natural to see if it can be generalized. It can indeed be generalized, though not uniformly for all algebras, the resulting formulae being dependent of the structure of the root systems. They are primarily based on the following basic observation.

Lemma 1. *Suppose that $x_1, x_2, \ldots, x_m$ are integers in $\mathbb{Z}\backslash n\mathbb{Z}$ satisfying $\sum_i x_i = \delta n \bmod 2n$, with $\delta = 0, 1$. Then*

$$\varepsilon_n(x_1)\varepsilon_n(x_2)\ldots\varepsilon_n(x_m) = (-1)^\delta \begin{Bmatrix} +1 \\ -1 \end{Bmatrix} \quad \textit{iff} \quad \sum_i \langle x_i\rangle_n = \begin{Bmatrix} 0 \\ n \end{Bmatrix} \bmod 2n. \tag{3.7}$$

Proof. Let μ be the number of indices i such that $\varepsilon_n(x_i) = -1$. Since for those is, $\langle x_i\rangle_n = \langle x_i\rangle_{2n} - n$, we obtain the following equalities modulo $2n$

$$\sum_i \langle x_i\rangle_n = \sum_i \langle x_i\rangle_{2n} - \mu n = (\delta + \mu)n \bmod 2n. \tag{3.8}$$

On the other hand, $\prod_i \varepsilon_n(x_i) = (-1)^\mu$, which proves the lemma. □

This simple result is the key to the generalization of (3.6). Let us first consider the algebras $su(N)$, for N odd. Recall that a positive root α of $su(N)$ has level $|\alpha| = l$ if α is the sum of l simple roots, and that the set of positive roots has the property that $\sum_{|\alpha|=l} \alpha = \sum_{|\alpha|=N-l} \alpha$.

For a weight $p = (a_1, a_2, \ldots, a_{N-1})$, the product formula (3.1) implies that the affine parity of p is the product of $su(2)$ parities $\varepsilon_n(\alpha \cdot p)$ over all positive roots. One can then satisfy the hypothesis of lemma 1 by replacing $\varepsilon_n(p \cdot \alpha)$ by $\varepsilon_n(n - p \cdot \alpha)$ for all positive roots of level bigger or equal to $(N + 1)/2$. Doing so, we obtain

$$\varepsilon_n(su(N); p) = \prod_{\substack{\alpha>0 \\ |\alpha|\leqslant(N-1)/2}} \varepsilon_n(p \cdot \alpha) \prod_{\substack{\alpha>0 \\ |\alpha|\geqslant(N+1)/2}} \varepsilon_n(n - p \cdot \alpha) \qquad N \text{ odd}. \tag{3.9}$$

The relevant value of δ is given by the number of positive roots whose level is bigger or equal to $(N + 1)/2$, namely $\delta = (N^2 - 1)/8 \bmod 2$. Thus, the lemma yields the following.

Proposition 1. *For $N \geqslant 3$ odd, one has*

$$\varepsilon_n(su(N); p) = (-1)^{(N^2-1)/8} \begin{Bmatrix} +1 \\ -1 \end{Bmatrix}$$

$$\textit{iff} \quad \sum_{\substack{\alpha>0 \\ |\alpha|\leqslant(N-1)/2}} \langle p \cdot \alpha\rangle_n + \sum_{\substack{\alpha>0 \\ |\alpha|\geqslant(N+1)/2}} \langle n - p \cdot \alpha\rangle_n = \begin{Bmatrix} 0 \\ n \end{Bmatrix} \quad \bmod 2n. \tag{3.10}$$

For $N = 3$, it reproduces (3.6) because the sum $\langle p \cdot \alpha_1\rangle_n + \langle p \cdot \alpha_2\rangle_n + \langle n - p \cdot (\alpha_1 + \alpha_2)\rangle_n$ can only take two values, n or $2n$.

The same trick does not always work for other algebras, because it relies on the fact that the positive roots can be partitioned into two sets such that the sum of the roots in one set equals the sum of the roots in the other set. In fact, it is not so much the roots which matter, but their scalar products with p. So the condition underlying this proposition is the existence of two disjoints sets A and B such that $\sum_{\alpha\in A} \alpha \cdot p = \sum_{\alpha\in B} \alpha \cdot p$. When this is not possible, there are two alternatives. Either one constrains the weight p so that it is possible, or one takes suitable multiples of the height n. We illustrate it in $su(4)$, which is the simplest case for which this occurs.

For $p = (a, b, c)$ a general weight of $su(4)$, the product formula yields

$$\varepsilon_n(su(4); p) = \varepsilon_n(a)\varepsilon_n(b)\varepsilon_n(c)\varepsilon_n(a + b)\varepsilon_n(b + c)\varepsilon_n(a + b + c). \tag{3.11}$$

One checks that if p is generic, there is no way to change some of the arguments as before, in such a way that they sum to a multiple of n. It is, however, possible if p is self-conjugate, $a = c$, since by inserting $\varepsilon_n^2(a) = 1$, one has

$$\varepsilon_n(su(4); p) = \varepsilon_n(b)\varepsilon_n(2a + b)\varepsilon_n^2(a) = \varepsilon_n(a)\varepsilon_n(a)\varepsilon_n(b)\varepsilon_n(n - 2a - b). \tag{3.12}$$

A simple application of the lemma implies, for a self-conjugate weight $p = (a, b, a)$, that

$$\varepsilon_n(su(4); p) = +1 \qquad \text{iff} \quad 2\langle a\rangle_n + \langle b\rangle_n + \langle n - 2a - b\rangle_n = n \bmod 2n. \tag{3.13}$$

If one wishes to keep a generic weight, the other way to proceed is to use the obvious identity $\varepsilon_n(x) = \varepsilon_{2n}(2x)$ and then to insert $\varepsilon_{2n}^2(a)\varepsilon_{2n}^2(c) = 1$ in (3.11)

$$\begin{aligned}\varepsilon_n(su(4);\, p) &= \varepsilon_{2n}(2a)\varepsilon_{2n}(2b)\varepsilon_{2n}(2c)\varepsilon_{2n}(2a+2b)\varepsilon_{2n}(2b+2c)\varepsilon_{2n}(2a+2b+2c)\varepsilon_{2n}^2(a)\varepsilon_{2n}^2(c)\\ &= \varepsilon_{2n}(2a)\varepsilon_{2n}(2b)\varepsilon_{2n}(2c)\varepsilon_{2n}(2a+2b)\varepsilon_{2n}(c)\varepsilon_{2n}(c)\\ &\quad\times\varepsilon_{2n}(2n-2b-2c)\varepsilon_{2n}(2n-2a-2b-2c)\varepsilon_{2n}(2n-a)\varepsilon_{2n}(2n-a). \end{aligned} \tag{3.14}$$

The lemma can be used once more to relate the affine parity of a general $su(4)$ weight to a sum of residues modulo $2n$. The price to pay is the larger number of residues that now enter the formulae.

For the other $su(N)$ algebras, N even, the first alternative (self-conjugate weights) works if $N = 0 \bmod 4$, while the second works well for all N even. Similar formulae can be designed for all other simple Lie algebras.

In the following two sections, we present some implications of the above multiplicative and additive formulae.

4. Totally positive numbers

For affine Lie algebras, the parity equation (2.14) requires that we determine the pairs of weights p, p' that satisfy the following parity equation

$$\varepsilon_n(\mathcal{G};hp)\varepsilon_n(\mathcal{G};hp') = \prod_{\alpha>0}\varepsilon_n(\alpha\cdot hp)\varepsilon_n(\alpha\cdot hp') = +1 \qquad \text{for all } h \text{ in } \mathbb{Z}_{nD}^*. \tag{4.1}$$

From the formula (2.17), this is equivalent to solving

$$\sigma_h\left(\prod_{\alpha>0}\sin\frac{\pi\alpha\cdot p}{n}\sin\frac{\pi\alpha\cdot p'}{n}\right) = \prod_{\alpha>0}\sin\frac{\pi h\alpha\cdot p}{n}\sin\frac{\pi h\alpha\cdot p'}{n} > 0 \qquad \forall h\in\mathbb{Z}_{nD}^*. \tag{4.2}$$

In other words, the positive algebraic real number within the brackets on the left-hand side must be such that its Galois conjugates are all positive. Such numbers are called totally positive. The previous equation can thus be interpreted by saying that $p, p' \in P_{++}(\mathcal{G})$ satisfy the parity rule iff $S_{\varrho,p}S_{\varrho,p'}$ is totally positive.

Obviously, sums, products and ratios of totally positive numbers are totally positive. A classical theorem about totally positive numbers is due to Landau and Hilbert (see, e.g. [12]).

Theorem 1. *A real algebraic number ξ is totally positive if and only if it is a sum of squares in $\mathbb{Q}(\xi)$.*

Proof. If ξ is a sum of squares, it is immediate that it is totally positive. Conversely, we assume that ξ is totally positive. Let $P(x)$ be the minimal polynomial of ξ

$$P(x) = x^n - a_1x^{n-1} + a_2x^{n-2} + \cdots + (-1)^n a_n. \tag{4.3}$$

Then the rational numbers a_i are all non-negative. The condition $P(\xi) = 0$ can be written

$$\xi(a_{n-1} + a_{n-3}\xi^2 + \cdots) = a_n + a_{n-2}\xi^2 + \cdots. \tag{4.4}$$

We set $\nu = a_{n-1} + a_{n-3}\xi^2 + \cdots$ and observe that $\nu \neq 0$ by the minimality of $P(x)$. Then we have

$$\xi = \frac{1}{\nu^2}(a_{n-1} + a_{n-3}\xi^2 + \cdots)(a_n + a_{n-2}\xi^2 + \cdots) = \frac{1}{\nu^2}(b_0 + b_1\xi^2 + \cdots) \tag{4.5}$$

where b_i are positive rationals. Since a positive rational is easily seen to be a sum of rational squares, the proof is complete. □

Thus, in order to solve the parity equation for affine algebras, we look for products of sines, in even number, which can be written as sums of squares in $\mathbb{Q}(\sin(\pi/n))$.

For n an integer and d a divisor of n, the identity $1 - X^d = \prod_{j=0}^{d-1}(1 - \zeta_d^j X)$ implies a number of product relations labelled by an integer a

$$\sin\frac{\pi ad}{n}\prod_{j=0}^{d-1}\sin\frac{\pi(a + jn/d)}{n} = 2^{1-d}\left(\sin\frac{\pi ad}{n}\right)^2 \qquad d \mid n \quad 1 \leqslant a \leqslant d-1. \tag{4.6}$$

The right-hand side is manifestly totally positive and so is the left-hand side

$$\sigma_h\left(\sin\frac{\pi ad}{n}\prod_{j=0}^{d-1}\sin\frac{\pi(a + jn/d)}{n}\right) > 0. \tag{4.7}$$

In order to convert this statement into identities involving parities, one simply remembers that $\sin(\pi x/n)$ lies in $\mathbb{Q}(\zeta_{4n})$†, so that the Galois group acts on it by

$$\sigma_h\left(\sin\frac{\pi x}{n}\right) = \mathrm{i}\sigma_h(-\mathrm{i})\sin\frac{\pi hx}{n} = \mathrm{i}\sigma_h(-\mathrm{i})\varepsilon_n(hx)\sin\frac{\pi\langle hx\rangle_n}{n}. \tag{4.8}$$

Thus, the positivity of a Galois conjugate is not only determined by an $su(2)$ parity, but can be affected by a sign $\mathrm{i}\sigma_h(-\mathrm{i})$. These signs (which depend on h) drop out when σ_h acts on an even number of sines, but otherwise give extra contributions when the number of sines is odd.

If d is odd, the number of sines is even, and (4.7) leads to identities between $su(2)$ parities

$$R_n(d,a) \equiv \varepsilon_n(had)\prod_{j=0}^{d-1}\varepsilon_n(ha + hjn/d) = +1 \qquad \forall h \in \mathbb{Z}_n^*,\ d \text{ odd}. \tag{4.9}$$

If d is even, we multiply the identity (4.6) by a positive rational sine, say $\sin(\pi f/n) \in \mathbb{Q}$, thereby preserving the total positivity. The resulting identities now involve an even number of sines and can be turned into identities among parities

$$R_n(d,a,f) \equiv \varepsilon_n(hf)\varepsilon_n(had)\prod_{j=0}^{d-1}\varepsilon_n(ha + hjn/d) = +1 \qquad \forall h \in \mathbb{Z}_n^*,\ d \text{ even}. \tag{4.10}$$

The allowed values $f = n/2$, $n/6$ and $5n/6$ are the only rationals such that $\sin(\pi f/n)$ is a strictly positive rational number.

Thus, we have succeeded in writing many identities $R_n(d,a)$ and $R_n(d,a,f)$ involving $su(2)$ parities, which can be used to give solutions to the parity equation in affine algebras. Here the main problem is precisely to recast these identities in the form (4.1), in which the arguments of the parities are related to the weights p, p' in a very specific way. It is nevertheless instructive to see how the known solutions of the parity equation can be understood in terms of these relations.

First, because the parity function for $\mathcal{G}$ is a product of parities for $su(2)$, one can solve the parity equation (4.1) by equating ε_n by pairs. These rather trivial solutions can lead to non-trivial couplings in terms of the weights, and it turns out that many apparently non-trivial couplings are in fact trivial in this sense. For instance in $su(5)$, it was found in [6], and checked the hard way, that the identity $p = (1,1,1,1)$ can couple, for even n, to the following three weights $p' = (1, (n/2)-2, (n/2)-2, 1)$, $((n/2)-3, 1, 1, (n/2)-3)$ and $((n/2)-3, 2, 2, (n/2)-3)$. To see that these three weights indeed satisfy the parity equation with p amounts to verifying, respectively, the identities

$$\varepsilon_n(2h)\varepsilon_n(n-2h)\varepsilon_n(4h)\varepsilon_n(n-4h) = +1 \qquad \forall h \tag{4.11}$$

$$\varepsilon_n(4h)\varepsilon_n(n-4h) = +1 \qquad \forall h \tag{4.12}$$

$$\varepsilon_n(2h)\varepsilon_n(n-2h) = +1 \qquad \forall h \tag{4.13}$$

† Indeed, $\sin(\pi x/n) = -\frac{1}{2}\mathrm{i}(\zeta_{2n}^{x} - \zeta_{2n}^{-x}) = -\frac{1}{2}(\zeta_{4n}^{2x+n} - \zeta_{4n}^{-2x+n})$.

simple consequences of the symmetry (2.18) of the function ε_n. These three couplings appear in the $su(5)$ exceptional invariants due to conformal embeddings, at heights $n = 8$, 10 and 12.

Many of the allowed couplings which are not trivial in the sense of the previous paragraph follow from the relations (4.9) and (4.10). For instance in $su(3)$ at height n, the coupling of $(1, 1)$ to $(1, (n/2))$ is allowed due to the identity

$$\varepsilon_n(h)\varepsilon_n(2h)\varepsilon_n(nh/2)\varepsilon_n((nh/2) + h) = +1 \tag{4.14}$$

which is the identity $R_n(2, 1, n/2)$. Similarly the coupling of $(1, 2)$ to $(2, (n/3) - 1)$ is a consequence of $R_n(3, 1)$. Aoki [7] has determined, for all integers n except 32 values between 3 and 180, all pairs p, p' of $su(3)$ weights which satisfy the parity equation. His result shows that, besides the trivial solutions, all the others follow from the identities (4.9) and (4.10) and products thereof. The same pattern holds in higher rank algebras and points to the genericity of the solutions provided by these identities. That they do not exhaust the solutions follows from a concrete example: in $su(3)$ at height $n = 15$, the weights $(1, 1)$ and $(1, 5)$ are allowed to couple, due to the identity

$$\varepsilon_{15}(h)\varepsilon_{15}(2h)\varepsilon_{15}(5h)\varepsilon_{15}(6h) = +1 \tag{4.15}$$

which does not seem to follow from the product relations R_n.

The use of these to solve parity equations for affine algebras remains a delicate matter, as subtle cancellations among individual parities must occur. A good (but still mild) illustration of this is provided by $su(4)$ at height $n = 14$, where there is a coupling between $(1, 1, 1)$ and $(1, 2, 7)$, due to three mechanisms: cancellations of pairs of identical ε_n, the symmetry $\varepsilon_n(x) = \varepsilon_n(n - x)$ and the relation $R_{14}(2, 2, 7)$.

5. Bernoulli numbers

In this section, we propose a second approach, based on the additive formulae of section 3. It is not entirely new, since the corresponding formula (3.6) for $su(3)$ was at the root of the works of Aoki [7] and Koblitz and Rohrlich [11]. With the additive formulae developed in section 3, the method can be extended to any affine algebra. The new feature that appears when one goes beyond $su(2)$ and $su(3)$, is the presence of congruences (all expressions are valued in a finite ring). As we shall see, this is the source of difficult arithmetical problems, which somehow embody the difficulties inherent to high-rank algebras.

Our purpose here is not to report on the results we have obtained so far by following this approach, since they are not conclusive at the moment. They do, however, suggest that this path is well suited for dealing with higher algebras. Here we will briefly explain the method and give an indication of the problems that arise. A detailed and more complete account will appear elsewhere.

The parity equation, expressing the equality of a number of parities $\varepsilon_n(\mathcal{G}; hp) = \varepsilon_n(\mathcal{G}; hp')$, is what we want to solve. The additive formulae, like those of proposition 1 in section 3, give an expression for each of these parities as a sum of residues modulo some integer. Thus, the typical problem is to find, for given and fixed n, all integers x_i, y_i satisfying

$$\sum_i \langle hx_i \rangle_n = \sum_i \langle hy_i \rangle_n \mod 2n \qquad \forall h \in \mathbb{Z}_n^*. \tag{5.1}$$

The integers x_i, y_i will eventually be related to the weights p and p' through their scalar products with positive roots of $\mathcal{G}$ (and so are not all independent).

The basic idea is to write equation (5.1) in the basis of characters of $\mathbb{Z}_n^*$, so we begin by recalling these.

Characters modulo n are homomorphisms of the multiplicative group $\mathbb{Z}_n^*$, i.e. they are multiplicative functions θ, satisfying $\theta(hh') = \theta(h)\theta(h')$ for all $h, h' \in \mathbb{Z}_n^*$ and of norm equal to 1. In concrete terms, if we write $\mathbb{Z}_n^* = \times_i Z_{m_i}$ as a product of cyclic groups, every element can be uniquely expressed as $h = \prod_i g_i^{t_i}$, with g_i a generator of Z_{m_i}. An arbitrary character is labelled by a set of integers a_i, adopting modulo m_i, and takes the simple form

$$\theta(h) = \zeta_{m_1}^{a_1 t_1} \zeta_{m_2}^{a_2 t_2} \ldots \qquad 0 \leqslant a_i \leqslant m_i - 1. \tag{5.2}$$

The character is even or odd depending on whether $\theta(-1) = +1$ or -1. If all m_i are chosen to be even integers, a character being even or odd means $\sum_i a_i = 0$ or 1 modulo 2.

A character of $\mathbb{Z}_n^*$ may be extended to $\mathbb{Z}_n$ (the set of all integers modulo n), by setting $\theta(t) = 0$ if t is not in $\mathbb{Z}_n^*$. If $n \mid N$, it may be further lifted to $\mathbb{Z}_N$ by periodicity modulo n (not forgetting the co-primality condition†), in which case we say that the resulting character of $\mathbb{Z}_N$ is induced by a character of $\mathbb{Z}_n$. A character of $\mathbb{Z}_n$ is called primitive if it is not induced by a character of a subgroup of $\mathbb{Z}_n$. A character modulo n is said to have conductor f if it is induced by a primitive character modulo f (so $f \mid n$). Loosely speaking, a character of conductor f truncates its argument modulo f and so the conductor of a character is its period.

Let us come back to the parity equation (5.1). It states that

$$\sum_i \langle hx_i \rangle_n - \sum_i \langle hy_i \rangle_n = 2nF(h \mid x_i, y_i) \tag{5.3}$$

for some integral function F. Because $\langle -x \rangle_n = n - \langle x \rangle_n$, the left-hand side is an odd function of h, and so is F. Multiplying by $\theta(h)$, a character modulo n, and summing over h yields zero if θ is an even character, while it gives a multiple of 2 if θ is odd‡. One obtains

$$\sum_i \sum_{h \in \mathbb{Z}_n^*} \langle hx_i \rangle_n \theta(h) - \sum_i \sum_{h \in \mathbb{Z}_n^*} \langle hy_i \rangle_n \theta(h) = 0 \mod 4n. \tag{5.4}$$

The change from a congruence modulo $2n$ to one modulo $4n$ is crucial for what follows.

It is important to realize that equation (5.4) takes place in the ring of integers of the cyclotomic extension $\mathbb{Q}(\zeta_{\varphi(n)})$ (containing the values of θ). Thus, the congruence involved is a condition in the finite ring $\mathbb{Z}(\zeta_{\varphi(n)})/(4n)$. By previous remarks, it is identically satisfied if θ is an even character, so from now on, we concentrate on the odd ones.

Equation (5.4) is a sum of terms of the form $\sum_h \langle hx \rangle_n \theta(h)$. Let us first compute this number when x is co-prime with n (invertible modulo n). For convenience, we include a factor $1/n$, and obtain, by a simple change of variable

$$\frac{1}{n} \sum_{h \bmod n} \langle hx \rangle_n \theta(h) = \frac{1}{n} \sum_{t \bmod n} \langle t \rangle_n \theta(x^{-1}t) = \theta^*(x) B_{1,\theta}^n \tag{5.5}$$

where $B_{1,\theta}^n$ is a generalized Bernoulli number (see [13])

$$B_{1,\theta}^n = \frac{1}{n} \sum_{t=1}^{n} t\theta(t). \tag{5.6}$$

If x is not co-prime with n, the calculation is only slightly more complicated. If we set $\mathrm{GCD}(x, n) = n/e$ and $\tilde{x} = x/(n/e)$ (so that $\tilde{x}$ is co-prime with e), a short calculation shows that for a character modulo n of conductor f, the sum is equal to

$$\frac{1}{n} \sum_{h \bmod n} \langle hx \rangle_n \theta(h) = \begin{cases} 0 & \text{if } f \nmid e \\ \dfrac{\varphi(n)}{\varphi(e)} B_{1,\theta}^e \theta^*(\tilde{x}) & \text{if } f \mid e. \end{cases} \tag{5.7}$$

† For instance, the character modulo 3 defined by $\theta(1) = 1$, $\theta(2) = -1$, can be extended modulo 6 by setting $\theta(1) = 1$, $\theta(5) = -1$.

‡ By this is meant that $\sum_h F(h \mid x_i, y_i)\theta(h)$ is an algebraic integer, lying in the principal ideal (2) of some cyclotomic integer ring.

Using these results, the parity equation in the form (5.4) is a congruence modulo 4 (we have divided by n) for a sum of terms comprising Bernoulli numbers, various factors related to GCDs, and values of characters. Instead of writing the complete equation in the general case, which does not pose a problem other than its notation, we take a simple example, and write it explicitly in the case of $su(4)$.

To simplify, we take in $su(4)$ two self-conjugate weights (a, b, a) and (a', b', a'), and assume that $a, b, 2a+b, a', b', 2a'+b'$ are all co-prime with n (this last assumption simplifies the notation, but is actually the most difficult situation). From (3.13), the congruences to solve are simple to write out

$$\tfrac{1}{2}B^n_{1,\theta}[2\theta^*(a)+\theta^*(b)-\theta^*(2a+b)-2\theta^*(a')-\theta^*(b')+\theta^*(2a'+b')] = 0 \bmod 2 \quad \text{for all odd } \theta. \tag{5.8}$$

Solving them requires looking more closely at the Bernoulli numbers.

As it turns out, Bernoulli numbers have received considerable attention for decades, because of the extremely important role they play in algebraic number theory. It would be an impossible task for us to review their properties. Instead, we will mention, without proof†, those which we feel are relevant for our problem.

A first observation is that the congruence (5.8) is between algebraic integers. The reason is very simple. The first congruence, equation (5.1), is the equality of two sums of residues, which are equal to 0 or to n modulo $2n$ (as follows from the lemma of section 3). However, since in any case, they are both equal to 0 modulo n, the congruence (5.1) is in fact trivial modulo n. When multiplied by $\theta(h)$ and summed over h, it yields (5.4), which must, therefore, be identically satisfied modulo $2n$. This means that equation (5.8) is identically satisfied modulo 1, i.e. that the left-hand side is an algebraic integer. Thus, the non-trivial part is entirely contained in a congruence modulo 2.

Technically, this observation is reflected by specific properties of the Bernoulli numbers $B^n_{1,\theta}$. Indeed, one can show that most of them are not only algebraic integers [14], despite the factor $1/n$ in their definition, but are also equal to 0 modulo 2. In other words, many numbers $\frac{1}{2}B^n_{1,\theta}$ are integral. The precise conditions under which this is true are not simple to state, but a sufficient condition is that the conductor of θ should not be a prime power‡.

When θ is such that $\frac{1}{2}B^n_{1,\theta}$ is integral, equation (5.8) simplifies further to become

$$\tfrac{1}{2}B^n_{1,\theta}[\theta^*(b)+\theta^*(2a+b)+\theta^*(b')+\theta^*(2a'+b')] = 0 \quad \bmod 2. \tag{5.9}$$

The main difficulty that arises when one tries to solve equations like (5.8) or the previous one, is to calculate the GCD of $\frac{1}{2}B^n_{1,\theta}$ and 2. Clearly the most favourable case is when the two numbers are co-prime, because one can then divide by $\frac{1}{2}B^n_{1,\theta}$ and study the conditions under which the sum of characters vanishes. Although that part may not be straightforward, we think it should be tractable, since it is merely a matter of having a certain sum of roots of unity that vanishes. Even if exotic solutions can occur, the generic solutions are expected to be the trivial ones, namely $a' = a$ and $b' = b$ (up to some automorphisms).

To see if half the Bernoulli numbers are co-prime with two, and if not, to calculate their GCD, is much more delicate. Even worse is the fact that they can vanish (as complex numbers). Indeed a standard identity gives the Bernoulli numbers associated to non-primitive characters

† For some of the results mentioned in the text, we have provided our own proof, although we have no doubt that they can be found somewhere in the mathematical literature.

‡ A particular instance where it is not true is when n is a power of an odd prime p. Then $B^n_{1,\theta}$ is not integral, but there is a unique prime ideal π in $\mathbb{Q}(\zeta_{\varphi(f)})$, lying above p, such that $\pi B^n_{1,\theta}$ is integral. In this situation, the triviality of the congruence modulo n is fulfilled because the various characters in (5.8) add up to something equal 0 modulo π.

in terms of those pertaining to primitive characters. If θ has conductor f and if θ_0 is the character modulo f that induces θ, then the formula is [13]

$$B^n_{1,\theta} = B^f_{1,\theta_0} \prod_{\text{prime}\, p|n} (1 - \theta_0(p)). \tag{5.10}$$

It is known that Bernoulli numbers associated with primitive characters are non-zero as complex numbers, so $B^f_{1,\theta_0} \neq 0$, but the product over the prime divisors of n may force a zero (this can only happen if n is not a prime power). As to the congruence modulo 2, $\frac{1}{2}B^n_{1,\theta}$ can have a common divisor with 2, either because $\frac{1}{2}B^f_{1,\theta_0}$ has one, or because $(1-\theta_0(p))$ divides 2 for some p. All these questions lead to rather non-trivial arithmetical problems in cyclotomic extensions.

It is, however, intriguing to note that the generalized Bernoulli numbers appear in a remarkable formula expressing what is called the relative class number h^- of cyclotomic fields. If h_n and h^+_n denote, respectively, the class number† of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\cos(2\pi/n))$, the relative class number of $\mathbb{Q}(\zeta_n)$ is their quotient, $h^-_n = h_n/h^+_n$. This number, also an integer, can be computed from the formula [13]

$$h^-_n = \tilde{Q} n \prod_{\substack{\theta \text{odd} \\ \text{primitive}}} \left(-\tfrac{1}{2}B^n_{1,\theta}\right) \tag{5.11}$$

where $\tilde{Q}$ is a numerical factor, equal to 1 if n is a power of 2, 2 if n is a odd prime power or if n is even, and 4 otherwise. From this formula, one can see that to determine the GCD of $\frac{1}{2}B^n_{1,\theta}$ and 2 amounts to say something about the power of 2 that divides the relative class number of cyclotomic fields. In this respect, Iwasawa's theory of $\mathbb{Z}_p$-extensions could provide some help.

Certainly, one cannot hide the fact that hard and maybe deep problems lie on the way towards the solution of the parity equation. However, one should emphasize that these problems, mostly concerned with Bernoulli numbers, are not specific to the $su(4)$ situation that we chose as illustration. If one follows the approach presented here, be it in $su(4)$ or in another algebra, one ends up with equations like (5.8) or (5.9), the solution of which requires basically two steps. One involves the Bernoulli numbers themselves, more precisely their modular properties; the other is an equation where certain values of characters add up to zero. Only this second part depends on which algebra we treat and which kind of weights. The first part is universal, algebra independent. This may be a happy coincidence as it is probably more difficult.

We can illustrate this by displaying the analogous equation‡ for $su(8)$, at height n. We make the same assumptions as for $su(4)$, namely we take two self-conjugate weights (a, b, c, d, c, b, a) and $(a', b', c', d', c', b', a')$. As before, we assume that all linear combinations of the Dynkin labels that appear are coprime with n. Then the equivalent of (5.9) involves a sum of only eight characters

$$\tfrac{1}{2}B^n_{1,\theta}[\theta^*(d) + \theta^*(2c+d) + \theta^*(2b+2c+d) + \theta^*(2a+2b+2c+d) + \text{same primed}] = 0 \mod 2 \tag{5.12}$$

valid for all odd characters which are such that $\frac{1}{2}B^n_{1,\theta}$ is integral.

† If $\mathbb{K}$ is a number field, i.e. a finite algebraic extension of $\mathbb{Q}$, the fractional ideals of $\mathbb{K}$ form an Abelian group, where the identity is just the ring of integers of $\mathbb{K}$. One defines an equivalence relation by saying that two ideals α and β are equivalent if $\alpha\beta^{-1}$ is principal (generated by a single element of $\mathbb{K}$). The quotient of the group of ideals by this relation is a finite group, called the ideal class group. Its order is the class number of $\mathbb{K}$ and is among the most important numbers characterizing $\mathbb{K}$.

‡ Interestingly, if we take two self-conjugate weights of $su(5)$, we obtain the same equation as for $su(4)$ (with b replaced by $2b$): the two weights $(a, 2b, a)$ and $(a', 2b', a')$ satisfy the parity equation for $su(4)$ if (a, b, b, a) and (a', b', b', a') satisfy the parity equation for $su(5)$. One easily convinces oneself that the same holds within all pairs of algebras $su(4\ell)$ and $su(4\ell+1)$, if one restricts to self-conjugate weights.

Without minimizing the difficulties, we believe that it is a very positive and encouraging feature of the approach presented here.

Acknowledgments

DA would like to thank the Institute for Theoretical Physics in Louvain-la-Neuve for the hospitality extended to him during visits. This work was completed whilst he was staying at the Institute of Theoretical Physics, ETH Zürich, and was supported by the Fonds National Suisse, both institutions are thanked. The authors also thank the referees for suggestions that have improved the paper's presentation and for pointing out some mistakes in the manuscript.

Appendix. Cohomological interpretations

In this appendix we study the parity functions as cohomological objects. We feel and hope that the cohomological interpretation can be useful in the future. In particular, we derive a formula relating the affine parities in *different* algebras, that has a strong cohomological flavour.

The parities, defined in the text by (2.8), satisfy the composition law

$$\varepsilon_{\sigma\sigma'}(j) = \varepsilon_\sigma(j)\varepsilon_{\sigma'}(\sigma(j)) = \varepsilon_{\sigma'}(j)\varepsilon_\sigma(\sigma'(j)) \tag{A.1}$$

where $\sigma, \sigma' \in \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$, and j labels the elements of $\mathcal{P}$, the finite set of chiral primary fields. The second equality follows from the fact that $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ is Abelian. We begin by reviewing some definitions of group cohomology, for which we adopt a multiplicative notation.

Let G be a group and A be a multiplicative Abelian group. Assume that G acts on A by automorphisms, i.e. there is a homomorphism $\alpha : G \to \mathrm{Aut}(A)$. For simplicity we write $g \cdot a$ instead of $\alpha(g)(a)$, where $g \in G$, $a \in A$. The set $C^n(G, A)$ of n-co-chains is the Abelian group of functions which depend on n variables in G and with values in A

$$C^n(G, A) = \{f : \underbrace{G \times \cdots \times G}_{n \text{ factors}} \to A\}. \tag{A.2}$$

By definition, a 0-co-chain is a fixed element of A, so that $C^0(G, A) = A$. One also defines co-boundary operators $\delta_n : C^n \to C^{n+1}$, which, for $n = 0, 1$, are given explicitly by

$$(\delta_0(a))(g) = (g \cdot a)a^{-1} \qquad g \in G \qquad a \in A, \tag{A.3}$$

$$(\delta_1(f))(g, h) = (g \cdot f(h))f(g)f(gh)^{-1} \qquad f \in C^1(G, A) \qquad g, h \in G. \tag{A.4}$$

The group of 1-co-boundaries is $B^1(G, A) = \mathrm{Im}(\delta_0)$, whereas the group of 1-co-cycles is $Z^1(G, A) = \ker(\delta_1)$. It is easy to see that $\delta_1 \circ \delta_0 = 1$, so $B^1(G, A) \subset Z^1(G, A)$. The first cohomology group is then $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

Now consider a RCFT with the finite set $\mathcal{P}$ of primary fields. Take $A = \{+1, -1\}^{\mathcal{P}}$ to be the multiplicative Abelian group of functions: $\mathcal{P} \to \{+1, -1\}$ (multiplication componentwise) and take $G = \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$. As recalled in the introduction, G acts on $\mathcal{P}$ by permutations $j \mapsto \sigma(j)$, and thus also on A by $(\sigma \cdot a)(j) = a(\sigma(j))$. The first equality in (A.1) then translates into the property that the map $\varepsilon : G \to A$ defined by $\sigma \mapsto \varepsilon_\sigma(\cdot)$ is a 1-co-cycle in $C^1(G, A)$.

Proposition 2. *If ε is a co-boundary, $\mathbb{M} = \mathbb{L}$.*

Proof. We know that $\mathrm{Gal}(\mathbb{M}/\mathbb{L})$ is the kernel of the restriction $\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, therefore, if $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{L})$, $\sigma(S_{ij}) = \varepsilon_\sigma(i)S_{ij}$, since the permutation of $\mathcal{P}$ induced by σ is determined by its restriction to $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. By the assumption on ε, $\varepsilon_\sigma(i) = a(\sigma(i))/a(i)$, for some $a \in A$, thus $\varepsilon_\sigma(i) = 1$ if $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{L})$. Hence $\sigma(S_{ij}) = S_{ij}$ for all $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{L})$. □

Examples of RCFTs where ε is a co-boundary include all models with the current algebra $su(N^2)$ at level 1. For these cases one easily checks that $\varepsilon_\sigma(p) = +1$ for all σ and all p in the alcove, and indeed $S_{\varrho,\varrho} = 1/N$ implies $\mathbb{M} = \mathbb{L}(S_{\varrho,\varrho}) = \mathbb{L}$. (Note that $\varepsilon_\sigma(\cdot)$ is the full parity defined in (2.8) and not the affine parity $\varepsilon_n(\mathcal{G};\cdot)$.) The converse is, however, not true: in models with current algebra $su(2)$ at even level, it is known that $\mathbb{M} = \mathbb{L}$ (see [9]) but ε is never a co-boundary†.

For $j \in \mathcal{P}$, we denote by $G_j = \{\sigma \in G \mid \sigma(j) = j\}$ the stabilizer of j. Note that since G is Abelian, $G_j = G_k$ if j and k belong to the same orbit $\mathcal{O}$ of G in $\mathcal{P}$, thus it makes sense to define the stabilizer of an orbit $\mathcal{O}$ by $G_\mathcal{O} = G_j$ with $j \in \mathcal{O}$. Let $\widehat{G}_\mathcal{O}$ be the group of homomorphisms $G_\mathcal{O} \to \{+1, -1\}$.

Proposition 3. *There is a group homomorphism $H^1(G, A) \hookrightarrow \prod_\mathcal{O} \widehat{G}_\mathcal{O}$, where the product is over all the orbits $\mathcal{O}$.*

The proof of proposition 3 is based on the following lemma.

Lemma 2. *ε is a co-boundary if and only if for all $j \in \mathcal{P}$ and all $\sigma \in G_j$, $\varepsilon_\sigma(j) = 1$.*

Proof. If we assume that ε is a co-boundary, then it is obvious that $\varepsilon_\sigma(j) = 1$ if $\sigma(j) = j$. Assume now that $\varepsilon_\sigma(j) = 1$ for all $\sigma \in G_j$. We have to construct a function $a(j)$ such that $\varepsilon_\sigma(j) = a(\sigma(j))/a(j)$.

First we observe that the co-cycle condition (A.1) implies that $\varepsilon_{\sigma\sigma'}(j) = \varepsilon_\sigma(j)$ if $\sigma' \in G_j$. Thus, if we restrict j to lie in a certain orbit $\mathcal{O}$, $\varepsilon_\sigma(j)$ depends only on $\sigma \bmod G_\mathcal{O}$ and we can think of σ as lying in $G/G_\mathcal{O}$.

Let us choose one particular element j_0 as the origin of $\mathcal{O}$. Every $j \in \mathcal{O}$ can be written in a unique way as $j = \sigma \cdot j_0$ for some $\sigma \in G/G_\mathcal{O}$. We define the restriction of a to $\mathcal{O}$ by $a(j) = \varepsilon_\sigma(j_0)$. From (A.1) we get

$$\varepsilon_{\sigma\sigma'}(j_0) = \varepsilon_{\sigma'}(j_0)\varepsilon_\sigma(\sigma' \cdot j_0) \tag{A.5}$$

so that upon setting $k = \sigma' \cdot j_0$, we get

$$\varepsilon_\sigma(k) = \varepsilon_{\sigma\sigma'}(j_0)/\varepsilon_{\sigma'}(j_0) = a(\sigma(k))/a(k). \tag{A.6}$$

□

Proof of proposition 3. We consider the second equality in (A.1) and assuming that $\sigma \in G_j$, we obtain $\varepsilon_\sigma(j) = \varepsilon_\sigma(\sigma' \cdot j)$. Therefore, if $\sigma \in G_\mathcal{O}$, $\varepsilon_\sigma(\cdot)$ is constant on $\mathcal{O}$. Denoting this constant by $\varepsilon_\sigma(\mathcal{O})$ it is easy to see from (A.1) again, that $\sigma \mapsto \varepsilon_\sigma(\mathcal{O})$ belongs to $\widehat{G}_\mathcal{O}$. Thus, we now have a map

$$\tilde{\varrho} : Z^1(G, A) \to \prod_\mathcal{O} \widehat{G}_\mathcal{O}. \tag{A.7}$$

The easy direction of the lemma says that $B^1(G, A) \subset \ker(\tilde{\varrho})$, so that $\tilde{\varrho}$ descends to a map

$$\varrho : H^1(G, A) \to \prod_\mathcal{O} \widehat{G}_\mathcal{O} \tag{A.8}$$

and the other direction says that in fact $B^1(G, A) = \ker(\tilde{\varrho})$, so that ϱ is injective. □

† The field extensions $\mathbb{M}$ and $\mathbb{L}$ have been determined in [10] for the current algebras based on $su(N)$. Many of them have $\mathbb{L} = \mathbb{M}$.

We finish by mentioning another product formula, relating the affine parities of $su(2N)$ and $su(2N+1)$. Formally, the formula says that the affine parity of $su(2N+1)$ is like the co-boundary of the affine parity of $su(2N)$, both algebras taken at the same height

$$\varepsilon_n(su(2N+1);(a_1,a_2,\ldots,a_{2N})) = `\ \delta_{2N-1}\varepsilon_n(su(2N);\cdot)\ ' \tag{A.9}$$

$$= \varepsilon_n(su(2N);(a_2,\ldots,a_{2N}))\prod_{i=1}^{2N-1}\varepsilon_n(su(2N);(a_1,\ldots,a_i+a_{i+1},\ldots,a_{2N})) \times\varepsilon_n(su(2N);(a_1,\ldots,a_{2N-1})). \tag{A.10}$$

It is only a formal co-boundary since, on $\mathbb{Z}^{2N-1}$, the parity $\varepsilon_n(su(2N);\cdot)$ takes the values $\{0,+1,-1\}$, which is not a multiplicative group. Nevertheless, in terms of affine parities, it yields an identity whose proof is straightforward: the two expressions are equal to +1 when $p=(a_1,a_2,\ldots,a_{2N})$ is in the alcove $P^n_{++}(su(2N+1))$ and they transform the same way under the affine Weyl group $\widehat{W}_n(su(2N+1))$. At this level of generality, these identities seem to be specific to the A_l series, even if other relations can be found. For instance, the $su(5)$ parity for a general weight is the product of four $su(3)$ parities, while a G_2 parity is the product of two $su(3)$ parities.

References

[1] Cardy J 1986 *Nucl. Phys.* B **270** 186–204
[2] Cappelli A, Itzykson C and Zuber J-B 1987 *Commun. Math. Phys.* **113** 1–26
Kato A 1987 *Mod. Phys. Lett.* A **2** 585–600
[3] Gannon T 1994 *Commun. Math. Phys.* **161** 233–64
[4] Kac V G 1990 *Infinite Dimensional Lie Algebras* 3rd edn (Cambridge: Cambridge University Press)
[5] Coste A and Gannon T 1994 *Phys. Lett.* B **323** 316–21
[6] Ruelle P, Thiran E and Weyers J 1993 *Nucl. Phys.* B **402** 693–708
[7] Aoki N 1991 *Am. J. Math.* **113** 779–833
[8] Bauer M, Coste A, Itzykson C and Ruelle P 1997 *J. Geom. Phys.* **22** 134–89
[9] Buffenoir E, Coste A, Lascoux J, Degiovanni P and Buhot A 1995 *Ann. Inst. Poincaré Theor. Phys.* **63** 41–79
[10] Gannon T and Walton M A On fusion algebras and modular matrices *Preprint* DAMTP–97–101, `q-alg/9709039`
[11] Koblitz N and Rohrlich D 1978 *Can. J. Math.* **30** 1183–205
[12] Siegel C L 1966–79 *Gesammelte Abhandlungen* Band I (Berlin: Springer)
[13] Washington L 1982 *Introduction to Cyclotomic Fields* (New York: Springer)
[14] Carlitz L 1959 *Bull. Math. Soc.* **65** 68–9