Journal of Algebra **217,** 496–527 (1999)
Article ID jabr.1998.7834, available online at http://www.idealibrary.com on IDEAL®

On Free Conformal and Vertex Algebras

Michael Roitman*

Communicated by Efim Zelmanov

Received April 1, 1998

Vertex algebras and conformal algebras have recently attracted a lot of attention due to their connections with physics and Moonshine representations of the Monster. See, for example, [6, 10, 17, 15, 19].

In this paper we describe bases of free conformal and free vertex algebras (as introduced in [6]; see also [20]).

All linear spaces are over a field $\Bbbk$ of characteristic 0. Throughout this paper $\mathbb{Z}_+$ will stand for the set of non-negative integers.

In Sections 1 and 2 we give a review of conformal and vertex algebra theory. All statements in these sections are either in [9, 17, 16, 15, 18, 20] or easily follow from results therein. In Section 3 we investigate free conformal and vertex algebras.

1. CONFORMAL ALGEBRAS

1.1. *Definition of Conformal Algebras*

We first recall some basic definitions and constructions; see [16, 15, 18, 20]. The main object of investigation is defined as follows:

DEFINITION 1.1. A *conformal algebra* is a linear space C endowed with a linear operator D: $C \to C$ and a sequence of bilinear products $\textcircled{n}$: $C \otimes C \to C$, $n \in \mathbb{Z}_+$, such that for any $a, b \in C$ one has

* Partially supported by NSF Grant DMS-9704132.

0021-8693/99 $30.00

(i) (Locality) There is a non-negative integer $N = N(a,b)$ such that $a \circled{n} b = 0$ for any $n \geq N$;

(ii) $D(a \circled{n} b) = (Da) \circled{n} b + a \circled{n} (Db)$;

(iii) $(Da) \circled{n} = -na \circled{n-1} b$.

1.2. *Spaces of Power Series*

Now let us discuss the main motivation for Definition 1.1. We closely follow [14, 18].

1.2.1. *Circle Products*

Let A be an algebra. Consider the space of power series $A[[z, z^{-1}]]$. We will write series $a \in A[[z, z^{-1}]]$ in the form

$$a(z) = \sum_{n \in \mathbb{Z}} a(n) z^{-n-1}, \qquad a(n) \in A.$$

On $A[[z, z^{-1}]]$ there is an infinite sequence of bilinear products $\circled{n}$, $n \in \mathbb{Z}_+$, given by

$$\big(a \circled{n} b\big)(z) = \operatorname{Res}_w\big(a(w)b(z)(z-w)^n\big). \tag{1.1}$$

Explicitly, for a pair of series $a(z) = \sum_{n \in \mathbb{Z}} a(n) z^{-n-1}$ and $b(z) = \sum_{n \in \mathbb{Z}} b(n) z^{-n-1}$ we have

$$\big(a \circled{n} b\big)(z) = \sum_m \big(a \circled{n} b\big)(m) z^{-m-1},$$

where

$$\big(a \circled{n} b\big)(m) = \sum_{s=0}^{n} (-1)^s \binom{n}{s} a(n-s) b(m+s). \tag{1.2}$$

There is also the linear derivation $D = d/dz$: $A[[z, z^{-1}]] \to A[[z, z^{-1}]]$. It is easy to see that D and $\circled{n}$ satisfy conditions (ii) and (iii) of Definition 1.1.

We can consider formula (1.2) as a system of linear equations with unknowns $a(k)b(l)$, $k \in \mathbb{Z}_+$, $l \in \mathbb{Z}$. This system is triangular, and its unique solution is given by

$$a(k)b(l) = \sum_{s=0}^{k} \binom{k}{s} \big(a \circled{s} b\big)(k+l-s). \tag{1.3}$$

Remark. The term "circle products" appears in [18], where the product "$\textcircled{n}$" is denoted by "$\circ_n$." In [15] this product is denoted by "$_{(n)}$."

1.2.2. *Locality*

Next we define a very important property of power series, which makes them form a conformal algebra. Let again A be an algebra.

DEFINITION 1.2 (See [1, 17, 15, 18, 20].) A series $a \in A[[z, z^{-1}]]$ is called *local of order N* to $b \in A[[z, z^{-1}]]$ for some $N \in \mathbb{Z}_+$ if

$$a(w)b(z)(z-w)^N = 0. \tag{1.4}$$

If a is local to b and b is local to a then we say that a and b are *mutually local*.

Remark. In [18, 20] the property (1.4) is called *quantum commutativity*.

Note that (1.4) implies that for every $n \geq N$ one has $a \textcircled{n} b = 0$. We will denote the order of locality by $N(a, b)$, i.e.,

$$N(a,b) = \min\left\{n \in Z_+ \mid \forall k \geq n, a \textcircled{k} b = 0\right\}.$$

Note also that if A is a commutative or skew-commutative or skew-commutative algebra, e.g., a Lie algebra, then locality is a symmetric relation. In this case we say "a and b are local" instead of "mutually local."

Let $a(z) = \sum_{m \in \mathbb{Z}} a(m) z^{-m-1}$ and $b(z) = \sum_{n \in \mathbb{Z}} b(n) z^{-n-1}$ be some series. Then the locality condition (1.4) reads

$$\sum_s (-1)^s \binom{N}{s} a(m-s)b(n+s) = 0 \qquad \text{for any } n, m \in \mathbb{Z}. \tag{1.5}$$

The locality condition (1.4) is known to be equivalent to the formula

$$a(m)b(n) = \sum_{s=0}^{N(a,b)-1} \binom{m}{s} (a \textcircled{s} b)(m+n-s). \tag{1.6}$$

The following statement is a trivial consequence of the definitions.

PROPOSITION 1.1. *Let A be an algebra and let $S \subset A[[z, z^{-1}]]$ be a space of pairwise mutually local power series, which is closed under all the circle products and ∂. Then S is a conformal algebra.*

One can prove (see, for example, [15]) that such families exhaust all conformal algebras.

Finally, we state here a trivial property of local series:

LEMMA 1.1. *Let* $a, b \in A[[z, z^{-1}]]$ *be a pair of formal power series and assume* a *is local to* b. *Then each of the series* a, Da, za *is local to each of* b, Db, zb.

1.3. *Construction of the Coefficient Algebra of a Conformal Algebra*

Given a conformal algebra C, we can build its *coefficient algebra* Coeff C in the following way. For each integer n take a linear space $\hat{A}(n)$ isomorphic to C. Let $\hat{A} = \oplus_{n \in \mathbb{Z}} \hat{A}(n)$. For an element $a \in C$ we will denote the corresponding element in $\hat{A}(n)$ by $a(n)$. Let $E \subset \hat{A}$ be the subspace spanned by all elements of the form

$$(Da)(n) + na(n-1) \qquad \text{for any } a \in C, n \in \mathbb{Z}. \tag{1.7}$$

The underlying linear space of Coeff C is $\hat{A}/E$. By an abuse of notation we will denote the image of $a(n) \in \hat{A}$ in Coeff C again by $a(n)$. The following proposition defines the product on Coeff C.

PROPOSITION 1.2. *Formula* (1.6) *unambiguously defines a bilinear product on* Coeff C.

Clearly (1.6) defines a product on $\hat{A}$. To show that the product is well defined on Coeff C, it is enough to check only that

$$(Da)(m)b(n) = -ma(m-1)b(n)$$

and

$$a(m)(Db)(n) = -na(m)b(n-1),$$

which is a straightforward calculation.

1.4. *Examples of Conformal Algebras*

1.4.1. *Differential Algebras*

Take a pair (A, δ), where A is an associative algebra and $\delta: A \to A$ is a locally nilpotent derivation,

$$\delta(ab) = \delta(a)b + a\delta(b), \qquad \delta^n(a) = 0 \qquad \text{for } n \gg 0.$$

Consider the ring $A[\delta, \delta^{-1}]$. Its elements are polynomials of the form $\sum_{i \in \mathbb{Z}} a_i \delta^i$, where only a finite number of $a_i \in A$ are nonzero. Here we put $a\delta^{-n} = a(\delta^{-1})^n$ and $a\delta^0 = a$. The multiplication is defined by the formula

$$a\delta^k \cdot b\delta^l = \sum_{i \geq 0} \binom{k}{i} a\delta^i(b)\delta^{k+l-i}.$$

It is easy to check that $A[\delta, \delta^{-1}]$ is a well-defined associative algebra. In fact, $A[\delta, \delta^{-1}]$ is the Ore localization of the ring of differential operators $A[\delta]$. If in addition A has an identity element 1, then $\delta(1) = 0$ and $\delta\delta^{-1} = \delta^{-1}\delta = 1$.

For $a \in A$ denote $\tilde{a} = \sum_{n\in\mathbb{Z}} a\delta^n z^{-n-1} \in A[\delta, \delta^{-1}][[z, z^{-1}]]$.

One easily checks that for any $a, b \in A$, $\tilde{a}$ and $\tilde{b}$ are local and

$$\tilde{a}\,\textcircled{n}\,\tilde{b} = \widetilde{a\delta^n(b)}. \tag{1.8}$$

So by Lemma 1.1 and Proposition 1.1 the series $\{\tilde{a} \mid a \in A\} \subset A[\delta, \delta^{-1}][[z, z^{-1}]]$ generate an (associative) conformal algebra; see Section 1.6.

One can instead consider $A[\delta, \delta^{-1}]$ to be a Lie algebra, with respect to the commutator $[p, q] = pq - qp$. If two series $\tilde{a}$ and $\tilde{b}$ are local in the associative sense they are local in the Lie sense, too. One computes also

$$\tilde{a}\,\textcircled{n}\,\tilde{b} = \widetilde{a\delta^n(b)} - \sum_{s\geq 0} (-1)^{n+s} \frac{1}{s!} \partial^s\big(b\delta^{n+s}(a)\big)^{\sim}, \tag{1.9}$$

where $\partial = d/dz$. Note that in (1.9) the circle products are defined by

$$\big(\tilde{a}\,\textcircled{n}\,\tilde{b}\big)(m) = \sum_{s=0}^{n} (-1)^s \binom{n}{s} [a\delta^{n-s}, b\delta^{m+s}]. \tag{1.10}$$

Again, it follows that $\{\tilde{a} \mid a \in A\} \subset A[\delta, \delta^{-1}][[z, z^{-1}]]$ generate a (Lie) conformal algebra; see Section 1.6.

An important special case is when there is an element $v \in A$ such that $\delta(v) = 1$. Then $\tilde{v} = \sum_n v\delta^n z^{-n-1} \in A[\delta, \delta^{-1}][[z, z^{-1}]]$ generates with respect to the product (1.10) a (centerless) Virasoro conformal algebra. It satisfies the relations

$$\tilde{v}\,\textcircled{0}\,\tilde{v} = \partial\tilde{v}, \qquad \tilde{v}\,\textcircled{1}\,\tilde{v} = 2\tilde{v},$$

and the rest of the products are 0.

1.4.2. *Loop Algebras*

Let $\mathfrak{g}$ be a Lie algebra over an algebraically closed field $\Bbbk$ and let σ: $\mathfrak{g} \to \mathfrak{g}$ be an automorphism of finite order, $\sigma^p = \mathrm{id}$. Then $\mathfrak{g}$ is decomposed into a direct sum of eigenspaces of σ:

$$\mathfrak{g} = \bigoplus_{k\in\mathbb{Z}/p\mathbb{Z}} \mathfrak{g}_k, \qquad \sigma|_{\mathfrak{g}_k} = e^{2\pi ik/p}.$$

Define a *twisted loop algebra* $\tilde{\mathfrak{g}} \subset \mathfrak{g} \otimes \Bbbk[t, t^{-1}]$ by

$$\tilde{\mathfrak{g}} = \left\{ \sum_j a_j t^j \,\middle|\, a_j \in \mathfrak{g}_{j \bmod p} \right\}.$$

The Lie product in $\tilde{\mathfrak{g}}$ is given by $[a \otimes t^m, b \otimes t^n] = [a, b] \otimes t^{m+n}$. If $p = 1$, then $\tilde{\mathfrak{g}} = \mathfrak{g} \otimes \Bbbk[t, t^{-1}]$, of course.

Now for any $a \in \mathfrak{g}_k$, $0 \le k < p$, define

$$\tilde{a} = \sum_{j \in \mathbb{Z}} a t^{pj+k} z^{-j-1} \in \tilde{\mathfrak{g}}[[z, z^{-1}]].$$

It is easy to see that any two $\tilde{a}, \tilde{b}$ are local with $N(\tilde{a}, \tilde{b}) = 1$ and if $a \in \mathfrak{g}_k$ and $b \in \mathfrak{g}_l$ we have

$$\tilde{a} \textcircled{0} \tilde{b} = \begin{cases} \widetilde{[a, b]} & \text{if } k + l < p, \\ z\widetilde{[a, b]} & \text{if } k + l \ge p. \end{cases}$$

As in Section 1.4.1, we conclude that $\{\tilde{a} \mid a \in \mathfrak{g}\} \subset \tilde{\mathfrak{g}}[[z, z^{-1}]]$ generate a (Lie) conformal algebra. Again, see Section 1.6 for the definition of varieties of conformal algebras.

1.5. *More on Coefficient Algebras*

Let C be a conformal algebra and let $A = \operatorname{Coeff} C$. Define

$$A_+ = \operatorname{Span}\{a(n) \mid a \in C, n \ge 0\},$$

$$A_- = \operatorname{Span}\{a(n) \mid a \in C, n < 0\},$$

$$A(n) = \operatorname{Span}\{a(n) \mid a \in C\}.$$

Define also for each $n \in \mathbb{Z}$ linear maps $\phi(n)$: $C \to A(n)$ by $a \mapsto a(n)$, and let $\phi = \sum_{n \in \mathbb{Z}} \phi(n) z^{-n-1}$: $C \to A[[z, z^{-1}]]$ so that $\phi a = \sum_{n \in \mathbb{Z}} a(n) z^{-n-1}$.

Here we summarize some general properties of conformal algebras and their coefficient algebras.

PROPOSITION 1.3. (a) $A = A_- \oplus A_+$ *is a direct sum of subalgebras.*

(b) A_+ *and* A_- *are filtered algebras with filtrations given by*

$$A(0) \subseteq A(1) \subseteq \cdots \subseteq A_+, \qquad A_- = A(-1) \supseteq A(-2) \supseteq \cdots,$$

$$\bigcup_{n \ge 0} A(n) = A_+, \qquad \bigcap_{n < 0} A(n) = 0.$$

(c) $$\operatorname{Ker} \phi(n) = \begin{cases} D^{n+1} C + \bigcup_{k \ge 1} \operatorname{Ker} D^k & \textit{if } n \ge 0, \\ \operatorname{Ker} D^{-n-1} & \textit{if } n < 0. \end{cases}$$

In particular, $\phi(-1)$ *is injective.*

(d) *The map* $\phi\colon C \to A[[z, z^{-1}]]$, *given by* $a \mapsto \sum_{n \in \mathbb{Z}} a(n) z^{-n-1}$, *is an injective homomorphism of conformal algebras*; *i.e., it preserves the circle products and agrees with the derivation*

$$\phi\big(a \textcircled{n} b\big) = \phi(a) \textcircled{n} \phi(b), \qquad \phi(Da) = D\phi(a). \tag{1.11}$$

(e) *The map* $\phi\colon C \to A[[z, z^{-1}]]$ *has the following universal property*: *For any homomorphism* $\psi\colon C \to B[[z, z^{-1}]]$ *of* C *to an algebra of formal power series, there is the unique algebra homomorphism* $\rho\colon A \to B$ *such that the corresponding diagram commutes*

$$\begin{array}{ccc} A\big[[z, z^{-1}]\big] & \xrightarrow{\ \rho\ } & B\big[[z, z^{-1}]\big] \\ {\scriptstyle\phi}\nwarrow & & \nearrow{\scriptstyle\psi} \\ & C & \end{array}$$

(f) *The formula* $D(a(n)) = -na(n-1)$ *defines a derivation* $D\colon A \to A$ *such that* $DA_- \subset A_-$, $DA_+ \subset A_+$.

Proof. From formula (1.6) for the product in A it easily follows that A_+ and A_- are indeed subalgebras. Also none of the linear identities (1.7) contains both generators with negative and non-negative index. This proves (a). Similar arguments establish also (b).

Now we prove that $\operatorname{Ker} \phi(n)$ is included in the right-hand side of (c). Take some $a \in C$, $a \neq 0$, and assume that $a(n) = 0$. Then $a(n) \in \hat{A}$ is a linear combination of identities (1.7) (see Section 1.3) so we must have in $\hat{A}$

$$a(n) = \sum_{k=k_{\min}}^{k_{\max}} \lambda_k\big((Da_k)(k) + ka_k(k-1)\big).$$

We can assume that $\lambda_k \neq 0$ for all $k_{\min} \leq k \leq k_{\max}$ and that $a_k \neq 0$ for $k = k_{\min}$ and for $k = k_{\max}$. Assume also that $\lambda_k = 0$ if $k > k_{\max}$ or $k < k_{\min}$.

Comparing terms with index k for $k_{\min} \leq k \leq k_{\max}$, we get

$$\delta_{kn} a = \lambda_k Da_k + \lambda_{k+1}(k+1) a_{k+1}. \tag{1.12}$$

Taking in (1.12) $k = k_{\min} - 1$, we see that there are two cases: Either (1) $k_{\min} = 0$ and $n \geq 0$ or (2) $n + 1 = k_{\min} \neq 0$.

Case 1. Taking in (1.12) $k = 0, \dots, n-1$, we get that $a_k \in D^k C$ for $0 \leq k \leq n$. Now we have two subcases: $k_{\max} > n$ and $k_{\max} \leq n$.

If $k_{\max} > n$ we substitute in (1.12) $k = k_{\max}, k_{\max} - 1, \dots, n + 1$ and get that $D^{k_{\max}-k+1}a_k = 0$. Now take $k = n$ in (1.12) and get that $a \in D^{n+1}C + \operatorname{Ker} D^{k_{\max}-n}$.

If $k_{\max} \leq n$ we have $\lambda_{n+1} = 0$, and hence substitution $k = n$ in (1.12) gives $a \in D^{n+1}C$.

Case 2. Here we again have two subcases: $n \geq 0$ or $n < 0$.

If $n \geq 0$ then, as in the previous case, we get $D^{k_{\max}-k+1}a_k = 0$ for $n + 1 \leq k \leq k_{\max}$. Now taking $k = n$ in (1.12), we get $a \in \operatorname{Ker} D^{k_{\max}-n}$.

Finally, if $n < 0$ then, since $\lambda_n = 0$, we have $a = \lambda_{n+1}(n+1)a_{n+1}$. Then we substitute $k = n + 1, n + 2, \dots$ into (1.12) until for some $k_0 \leq -1$ we get $\lambda_{k_0+1}(k_0 + 1)a_{k_0+1} = 0$. It follows that $D^{k_0-k+1}a_k = 0$ for $n + 1 \leq k \leq k_0$; therefore $a \in \operatorname{Ker} D^{k_0-n} \subset \operatorname{Ker} D^{-n-1}$. This proves one inclusion in (c). It also follows that $\operatorname{Ker} \phi(-1) = 0$.

Next we show that ϕ is a homomorphism of conformal algebras, that is, formulas (1.11) hold. For the first identity we have

$$\begin{aligned}\phi(Da) &= \sum_{n\in\mathbb{Z}} (Da)(n) z^{-n-1} = \sum_{n\in\mathbb{Z}} (-n) a(n-1) z^{-n-1}\\ &= \frac{d}{dz}\sum_n a(n) z^{-n-1}.\end{aligned}$$

The second identity reads

$$\big(a\,\textcircled{n}\,b\big)(m) = \sum_s (-1)^s \binom{n}{s} a(n-s) b(m+s),$$

which is precisely the formula (1.2).

Now (d) is done after we notice that ϕ is injective, since $\phi(-1)$ is injective.

Now we can prove the other inclusion in (c). If $a \in \operatorname{Ker} D^k C$, then ϕa is a solution of the differential equation $\partial_z^k \phi a(z) = 0$. Hence ϕa is a polynomial of degree at most $k - 1$, and therefore $\phi(n)a = 0$ for $n \geq 0$ and for $n < -k$. If $a \in D^k C$, then $\phi(n)a = 0$ for $0 \leq n \leq k - 1$, by induction and (1.7).

Statement (e) is clear, since identities (1.7) hold for any homomorphism $\psi\colon C \to B[[z, z^{-1}]]$.

Finally, the formula $D(a(n)) = -na(n-1)$ defines a derivative of $\hat{A}$. So in order to prove (f) we have to show that D agrees with the identities (1.7). This is indeed the case:

$$D((Da)(n) + na(n-1)) = -n((Da)(n-1) + (n-1)a(n-2)).$$

∎

1.6. *Varieties of Conformal Algebras*

Consider now a variety of algebras $\mathfrak{A}$ (see [8, 13]).

DEFINITION 1.3. A conformal algebra C is a $\mathfrak{A}$-*conformal algebra* if $\operatorname{Coeff} C$ lies in the variety $\mathfrak{A}$.

The identities in $\mathfrak{A}$-conformal algebras are all the circle product identities R such that for any integer m, $R(m)$ becomes an $\mathfrak{A}$-algebra identity after substitution of (1.2) for every circle product in R. Conversely, given a classical algebra identity r, we can substitute (1.6) for all products in r and get an identity of $\mathfrak{A}$-conformal algebras. This way we get a correspondence between classical and conformal identities. See the next section for examples.

Combining Propositions 1.1 and 1.3(d), we get the following well-known fact:

PROPOSITION 1.4. *$\mathfrak{A}$-conformal algebras are exhausted (up to isomorphism) by conformal algebras of formal power series $S \subset A[[z, z^{-1}]]$ for $\mathfrak{A}$-algebras A.*

1.7. *Associative and Lie Conformal Algebras*

The following theorem gives the explicit correspondence between conformal and classical algebras in some important cases.

THEOREM 1.1 [16]. *Let C be a conformal algebra and let $A = \operatorname{Coeff} C$ be its coefficient algebra.*

(a) *A is associative if and only if the following identity holds in C:*

$$\left(a \textcircled{n} b\right) \textcircled{m} c = \sum_{s=0}^{n} (-1)^s \binom{n}{s} a \textcircled{$n-s$} \left(b \textcircled{$m+s$} c\right). \tag{1.13}$$

(b) *The Jacoby identity $[[a, b], c] = [a, [b, c]] - [b, [a, c]]$ in A is equivalent to the following conformal Jacoby identity in C:*

$$\left(a \textcircled{n} b\right) \textcircled{m} c = \sum_{s=0}^{n} (-1)^s \binom{n}{s} \times \left(a \textcircled{$n-s$} \left(b \textcircled{$m+s$} c\right) - b \textcircled{$m+s$} \left(a \textcircled{$n-s$} c\right)\right). \tag{1.14}$$

(c) *The skew-commutativity identity* $[a, b] = -[b, a]$ *in* A *corresponds to the quasi-symmetry identity*

$$a \circled{n} b = \sum_{s \geq 0} (-1)^{n+s+1} \frac{1}{s!} D^s (b \circled{n+s} a). \tag{1.15}$$

(d) *The commutativity of* A *is equivalent to*

$$a \circled{n} b = \sum_{s \geq 0} (-1)^{n+s} \frac{1}{s!} D^s (b \circled{n+s} a). \tag{1.16}$$

The identities (1.13), (1.14), and (1.15) immediately imply the following:

COROLLARY 1.1. *Let* C *be a Lie conformal or an associative conformal algebra and let* $A = \operatorname{Coeff} C$ *be its coefficient algebra. Then* C *is an* A_+*-module with the action given by* $a(n)c = a \circled{n} c$ *for* $a, c \in C$, $n \in \mathbb{Z}_+$. *Moreover, this action agrees with the derivations on* A_+ *and* C: $(Da(n))c = [D, a(n)]c$.

From now on we will deal only with associative or Lie conformal algebras.

1.8. *Dong's Lemma*

We end this section by stating a very important property of formal power series over associative or Lie algebras. This property allows us to construct conformal algebras by taking a collection of generating series.

LEMMA 1.2. *Let* A *be an associative or a Lie algebra and let* $a, b, c \in A[[z, z^{-1}]]$ *be three formal power series. Assume that they are pairwise mutually local. Then for all* $n \in \mathbb{Z}_+$, $a \circled{n} b$ *and* c *are mutually local. Moreover, in the Lie algebra case,*

$$N(a \circled{n} b, c) = N(c, a \circled{n} b) \leq N(a, b) + N(b, c) + N(c, a) - n - 1, \tag{1.17}$$

and, in the associative case,

$$N(a \circled{n} b, c) \leq N(b, c), \qquad N(c, a \circled{n} b) \leq N(c, a) + N(a, b) - n - 1.$$

2. VERTEX ALGEBRAS

2.1. *Fields*

Let now V be a vector space over $\Bbbk$. Denote by $gl(V)$ the Lie algebra of all $\Bbbk$-linear operators on V. Consider the space $\mathrm{F}(V) \subset gl(V)[[z, z^{-1}]]$ of *fields* on V, given by

$$\mathrm{F}(V) = \left\{ \sum_{n \in \mathbb{Z}} a(n) z^{-n-1} \middle| \forall v \in V, a(n)v = 0 \text{ for } n \gg 0 \right\}.$$

For $a(z) \in \mathrm{F}(V)$ denote

$$a_-(z) = \sum_{n<0} a(n) z^{-n-1}, \qquad a_+(z) = \sum_{n \geq 0} a(n) z^{-n-1}.$$

Denote also by $\mathbb{1} = \mathbb{1}_{\mathrm{F}(V)} \in \mathrm{F}(V)$ the identity operator, such that $\mathbb{1}(-1) = \mathrm{Id}_V$; all other coefficients are 0.

Remark. In [18, 20] the elements of $\mathrm{F}(V)$ are called *quantum operators* on V.

We view $gl(V)$ as a Lie algebra, and Section 1.2.1 gives a collection of products $\textcircled{n}$, $n \in \mathbb{Z}_+$, on $\mathrm{F}(V)$. Now in addition to these products we introduce products $\textcircled{n}$ for $n < 0$. Define first $\textcircled{-1}$ by

$$a(z) \textcircled{-1} b(z) = a_-(z) b(z) + b(z) a_+(z). \tag{2.1}$$

Note that the products in (2.1) make sense, since for any $v \in V$ we have $a(n)v = b(n)v = 0$ for $n \gg 0$. The -1st product is also known as the *normally ordered product* (or *Wick product*) and is usually denoted by $:a(z)b(z):$.

Next, for any $n < 0$ set

$$a(z) \textcircled{n} b(z) = \frac{1}{(-n-1)!} :\big(D^{-n-1} a(z)\big) b(z):, \tag{2.2}$$

where $D = \frac{d}{dz}$. Taking $b = \mathbb{1}$, we get

$$a \textcircled{-1} \mathbb{1} = a, \qquad a \textcircled{-2} \mathbb{1} = Da. \tag{2.3}$$

It is easy to see that

$$\mathbb{1} \textcircled{n} a = \delta_{-1,n} a.$$

We have the following explicit formula for the circle products: If $(a \textcircled{n} b)(z) = \sum_m (a \textcircled{n} b)(m) z^{-m-1}$, then

$$\left(a \textcircled{n} b\right)(m) = \sum_{s \le n} (-1)^{s+n} \binom{n}{n-s} a(s) b(m+n-s) - \sum_{s \ge 0} (-1)^{s+n} \binom{n}{s} b(m+n-s) a(s). \tag{2.4}$$

Note that if $n > 0$ then (2.4) becomes

$$\left(a \textcircled{n} b\right)(m) = \sum_{s \ge 0} (-1)^{n+s} \binom{n}{s} \left[a(s), b(m+n-s)\right],$$

which is precisely formula (1.2) for Lie algebras.

It is easy to see that D is a derivation of all the circle products:

$$D\left(a \textcircled{n} b\right) = Da \textcircled{n} b + a \textcircled{n} Db. \tag{2.5}$$

Note also that the Dong's Lemma 1.2 remains valid for negative n and the estimate (1.17) still holds.

2.2. *Definition of Vertex Algebras*

Instead of giving a formal definition of a vertex algebra in the spirit of Definition 1.1, we present a description of these algebras similar to Proposition 1.4. For a more abstract approach see, e.g., [9, 15, 18, 20].

DEFINITION 2.1. A *vertex algebra* is a subspace $S \subset \mathrm{F}(V)$ of fields over a vector space V such that

(i) Any two fields $a, b \in S$ are local (in the Lie sense).

(ii) S is closed under all the circle products $\textcircled{n}$, $n \in \mathbb{Z}$, given by (2.4).

(iii) $\mathbb{1} \in S$.

Note that from (2.3) it follows that a vertex algebra is closed under the derivation $D = d/dz$.

Note also that a vertex algebra is a Lie conformal algebra.

Let $S \subset \mathrm{F}(V)$ be a vertex algebra. We introduce the left action map Y: $S \to \mathrm{F}(S)$ defined by

$$Y(a) = \sum_{n \in \mathbb{Z}} \left(a \textcircled{n} \cdot\right) \zeta^{-n-1}. \tag{2.6}$$

Clearly, $Y(\mathbb{1}_S) = \mathbb{1}_{\mathrm{F}(S)}$.

We state here the following characterizing property of Y (see [15, 20]):

PROPOSITION 2.1. *The left action map* $Y\colon S \to \mathrm{F}(S)$ *is an isomorphism of vertex algebras, i.e.,* $Y(S) \subset \mathrm{F}(S)$ *is a vertex algebra and*

$$Y\big(a \,\textcircled{n}\, b\big) = Y(a) \,\textcircled{n}\, Y(b), \qquad Y(\mathbb{1}_S) = \mathbb{1}_{\mathrm{F}(S)}. \tag{2.7}$$

From (2.3) and (2.5) it follows that Y also agrees with D:

$$Y(Da) = \partial_\zeta Y(a) = \left[D, Y(a)\right].$$

2.3. *Enveloping Vertex Algebras of a Lie Conformal Algebra*

Let C be a Lie conformal algebra and let $L = \operatorname{Coeff} C$ be its coefficient Lie algebra.

DEFINITION 2.2 [14, 15]. (a) An L-module M is called *restricted* if for any $a \in C$ and $v \in M$ there is some integer N such that for any $n \geq N$ one has $a(n)v = 0$

(b) An L-module M is called a *highest weight* module if it is generated over L by a single element $m \in M$ such that $L_+ m = 0$. In this case m is called the *highest weight vector*.

Clearly any submodule and any factor module of a restricted module are restricted.

Let M be a restricted L-module. Then the representation $\rho\colon L \to gl(M)$ could be extended to the map $\rho\colon L[[z, z^{-1}]] \to \mathrm{F}(M)$ which combined with the canonical embedding $\phi\colon C \to L[[z, z^{-1}]]$ (see Proposition 1.3)(d) gives a conformal algebra homomorphism $\psi\colon C \to \mathrm{F}(M)$. Then $\psi(C) \subset \mathrm{F}(M)$ consists of pairwise local fields, and by Dong's Lemma 1.2, $\psi(C)$ together with $\mathbb{1} \in \mathrm{F}(M)$ generates a vertex algebra $S_M \subset F(M)$.

The following proposition is well known; see, e.g., [11].

PROPOSITION 2.2. (a) *The vertex algebra* $S = S_M$ *has the structure of a highest weight module over* L *with the highest weight vector* $\mathbb{1}$. *The action is given by*

$$a(n)\,\beta = \psi(a) \,\textcircled{n}\, \beta, \qquad a \in C, n \in \mathbb{Z}, \beta \in S_M.$$

Moreover this action agrees with the derivations:

$$\big(Da(n)\big)\,\beta = \left[D, a(n)\right]\beta.$$

(b) *Any* L*-submodule of* S *is a vertex algebra ideal. If* M_1 *and* M_2 *are two restricted* L*-modules,* $S_1 = S_{M_1}$, $S_2 = S_{M_2}$, *and* $\mu\colon S_1 \to S_2$ *is an* L*-mod-*

ule homomorphism such that $\mu(\mathbb{1}) = \mathbb{1}$, *then* μ *is a vertex algebra homomorphism.*

2.4. *Universal Enveloping Vertex Algebras*

Now we build a universal highest weight module V over L, which is often referred to as a *Verma module*. Take the one-dimensional trivial L_+-module $\Bbbk\, \mathbb{1}_V$, generated by an element $\mathbb{1}_V$. Then let

$$Y = \operatorname{Ind}_{L_+}^{L} \Bbbk\, \mathbb{1}_V = U(L) \otimes_{U(L_+)} \Bbbk\, \mathbb{1}_V \cong U(L)/U(L)L_+ .$$

It is easy to see that V is a restricted module and hence we get an enveloping vertex algebra $S = S_V \subset \mathrm{F}(V)$ and a homomorphism $\psi: C \to S$. Clearly, ψ is injective, since $\rho: L \to gl(V)$ is injective.

THEOREM 2.1. (a) *The map* $\chi: S \to V$ *given by* $\alpha \mapsto \alpha(-1)\mathbb{1}_V$ *is an* L*-module isomorphism, and* $\chi(\mathbb{1}_S) = \mathbb{1}_V$.

(b) S *is the universal enveloping vertex algebra of* C *in the following sense: If* $\mu: C \to U$ *is another homomorphism of* C *to a vertex algebra* U, *then there is the unique map* $\hat{\mu}: S \to U$ *which makes up the following commutative triangle*:

$$\begin{array}{ccc} S & \xrightarrow{\hat{\mu}} & U \\ \nwarrow_{\psi} & & \nearrow_{\mu} \\ & C & \end{array}$$

From now on we identify V and $S = S_V$ via χ and write $V = V(C)$ for the universal enveloping vertex algebra of a Lie conformal algebra C and $\mathbb{1}_S = \mathbb{1}_V = \mathbb{1}$. The embedding $\psi: C \to V = U(L)/U(L)L_+$ is then given by $a \mapsto a(-1)\mathbb{1}$. By Proposition 1.3(c), the map $\phi(-1): C \to L_-$, defined by $a \mapsto a(-1)$, is an isomorphism of linear spaces. Therefore, the image of C in V is equal to $\psi(C) = L_- \mathbb{1} = L\mathbb{1} \subset V$.

3. FREE CONFORMAL ALGEBRAS

3.1. *Definition of Free Conformal and Free Vertex Algebras*

Let $\mathscr{B}$ be a set of symbols. Consider a function $N: \mathscr{B} \times \mathscr{B} \to \mathbb{Z}_+$, which will be called a *locality function*.

Let $\mathfrak{A}$ be a variety of algebras. In all the applications $\mathfrak{A}$ will be either Lie or associative algebras. Consider the category $\mathfrak{Conf}(N)$ of $\mathfrak{A}$-conformal algebras (see Section 1.6) generated by the set $\mathscr{B}$ such that in any conformal algebra $C \in \mathfrak{C}onf(N)$ one has

$$a \textcircled{n} b = 0 \qquad \forall a, b \in \mathcal{B}\ \forall n \geq N(a, b).$$

By an abuse of notation we will not make a distinction between $\mathcal{B}$ and its image in a conformal algebra $C \in \mathfrak{C}onf(N)$.

The morphisms of $\mathfrak{Conf}(N)$ are, naturally, conformal algebra homomorphisms f: $C \to C'$ such that $f(a) = a$ for any $a \in \mathcal{B}$.

We claim that $\mathfrak{Conf}(N)$ has the universal object, a conformal algebra $C = C(N)$, such that for any other $C' \in \mathfrak{Conf}(N)$ there is the unique morphism f: $C \to C'$. We call $C(N)$ a *free conformal algebra*, corresponding to the locality function N.

In order to build $C(N)$, we first build the corresponding coefficient algebra $A = \operatorname{Coeff} C$ (see Section 1.3).

Let $A \in \mathfrak{A}$ be the algebra presented by the set of generators

$$X = \{b(n) \mid b \in \mathcal{B}, n \in \mathbb{Z}\} \tag{3.1}$$

with relations

$$\left\{ \sum_s (-1)^s \binom{N(b,a)}{s} b(n-s)a(m+s) = 0 \,\middle|\, a, b \in \mathcal{B}, m, n \in \mathbb{Z} \right\}. \tag{3.2}$$

For any $b \in \mathcal{B}$ let $\tilde{b} = \sum_n b(n) z^{-n-1} \in A[[z, z^{-1}]]$. From (3.2) it follows that any two $\tilde{a}$ and $\tilde{b}$ are mutually local; therefore by Dong's Lemma 1.2 they generate a conformal algebra $C \subset A[[z, z^{-1}]]$.

PROPOSITION 3.1. (a) $A = \operatorname{Coeff} C$.

(b) *The conformal algebra C is the free conformal algebra corresponding to the locality function N.*

Proof. (a) Clearly, there is a surjective homomorphism $A \to \operatorname{Coeff} C$, since relations (3.2) must hold in $\operatorname{Coeff} C$. Now the claim follows from the universal property of $\operatorname{Coeff} C$ (see Proposition 1.3(e)).

(b) Take another algebra $C' \in \mathfrak{Conf}(N)$ and let $A' = \operatorname{Coeff} C'$. Obviously, there is an algebra homomorphism f: $A \to A'$ such that $f(b(n)) = b(n)$ for any $b \in \mathcal{B}$ and $n \in \mathbb{Z}$. It could be extended to a map f: $A[[z, z^{-1}]] \to A'[[z, z^{-1}]]$. Now it is easy to see that the restriction $f|_C$

gives the desired conformal algebra homomorphism $C \to C'$:

$$\begin{array}{ccc} A[[z, z^{-1}]] & \xrightarrow{f} & A'[[z, z^{-1}]] \\ \uparrow & & \uparrow \\ C & \xrightarrow{f} & C' \end{array}$$

Indeed, due to formula (1.2), f preserves the circle products, and, since ∂ is a derivation of the products, and $f(\partial\tilde{a}) = \partial f(\tilde{a})$, for $a \in C$ one has $f(\partial\phi) = \partial f(\phi)$ for any $\phi \in C$. ∎

In the case when $\mathfrak{A}$ is the variety of Lie algebras, we may consider the universal vertex enveloping algebra $V(C)$ of a free Lie conformal algebra $C = C(N)$. In accordance with Theorem 2.1, we call $V(C)$ a *free vertex algebra*.

Though the construction of free conformal and vertex algebras makes sense for an arbitrary locality function $N: \mathscr{B} \times \mathscr{B} \to \mathbb{Z}_+$, the results of Sections 3.4–3.7 are valid only for the case when N is constant.

3.2. *The Positive Subalgebra of* Coeff $C(N)$

Let again $C = C(N)$ be a free conformal algebra corresponding to a locality function $N: \mathscr{B} \times \mathscr{B} \to \mathbb{Z}_+$, $\mathscr{B}$ being an alphabet, and let $A =$ Coeff C. Recall that by Proposition 1.3(a) we have the decomposition $A = A_- \oplus A_+$ of the coefficient algebra into the direct sum of two subalgebras. Denote $X_i = \{b(n) \mid b \in \mathscr{B}, n \geq i\} \subset X$.

LEMMA 3.1. *The subalgebra $A_+ \subset A$ is isomorphic to the algebra $\hat{A}_+$ presented by the set of generators X_0 and those of relations* (3.2) *which contain only elements of X_0*:

$$\left\{ \sum_s (-1)^s \binom{N(b,a)}{s} b(n-s)a(m+s) = 0 \,\middle|\, a, b \in \mathscr{B}, m \geq 0, \right.$$
$$\left. n \geq N(b,a) \right\}. \qquad (3.3)$$

Proof. Clearly, there is a surjective homomorphism $\varphi: \hat{A}_+ \to A_+$ which maps X_0 to itself. We prove that φ is in fact an isomorphism. We proceed in four steps.

Step 1. First we prove that A_+ is generated by X_0 in A. Indeed, we have $X_0 \subset A_+$. On the other hand, A_+ is spanned by elements of the form

$a(m)$, where $m \geq 0$ and $a \in C$ is a circle product monomial in $\mathscr{B}$. By induction on the length of a it is enough to check that if $a = a_1 \textcircled{k} a_2$, then $a(m)$ is in the subalgebra, generated by X_0, which follows from (1.2).

Step 2. Let $\hat{\tau}$: $\hat{A}_+ \to \hat{A}_+$ be the homomorphism, which acts on the generators X_0 by $a(n) \mapsto a(n+1)$, so that $\hat{\tau}(\hat{A}_+)$ is the subalgebra of $\hat{A}_+$ generated by X_1. We claim that $\hat{\tau}$ is injective, and therefore $\hat{\tau}(\hat{A}_+) \cong \hat{A}_+$. Indeed, $\hat{\tau}$ acts on the free associative algebra $\Bbbk\langle X_0 \rangle$. Assume that for some $p \in \hat{A}_+$ we have $\hat{\tau}(p) = 0$. Take any preimage $P \in \Bbbk\langle X_0 \rangle$ of p. Then we have $\hat{\tau}(P) = \sum_i \xi_i R_i$, where $\xi_i \in \Bbbk\langle X_0 \rangle$ and R_i are relations (3.3), such that in all ξ_i and R_i there appear only indexes greater than or equal to 1. But then P itself must be of the form $\sum_i \xi_i' R_i'$, where "$'$" stands for decreasing all indexes by 1; hence $p = 0$.

Step 3. Next we claim that there is an automorphism τ of the algebra A which acts on the generators X by the shift $a(n) \mapsto a(n+1)$. Indeed, relations (3.2) are invariant under the shift, and clearly, τ is invertible. For any integer n denote $A_n = \tau^n A_+$. We have $A_n \cong A_+ = A_0$ for every n.

Step 4. Now for each integer n take a copy $\hat{A}_n$ of $\hat{A}_+$. Let $\hat{\tau}_n$: $\hat{A}_n \to \hat{A}_{n-1}$ be the isomorphism of $\hat{A}_+$ onto $\hat{\tau}(\hat{A}_+)$, built in Step 1. Let $\hat{A}$ be the limit of all these $\hat{A}_n$ with respect to the maps $\hat{\tau}_n$. We identify generators of $\hat{A}_n$ with the set X_n. It is easy to see that φ: $\hat{A}_0 \to A_0$ extends to the homomorphism φ: $\hat{A} \to A$, such that $\varphi(\hat{A}_n) = A_n$ and $\varphi|_X = \mathrm{id}$. Now we observe that all the defining relations (3.2) of A hold in $\hat{A}$; hence there is an inverse map φ^{-1}: $A \to \hat{A}$, and therefore φ is an isomorphism. ▮

3.3. *The Diamond Lemma*

For future purposes we need a digression on the diamond lemma for associative algebras. We closely follow [2], but use more modern terminology.

Let X be some alphabet and let K be some commutative ring. Consider the free associative algebra $K\langle X \rangle$ of non-commutative polynomials with coefficients in K. Denote by X^* the set of words in X, i.e., the free semigroup with 1 generated by X.

A *rule* on $K\langle X \rangle$ is a pair $\rho = (w, f)$, consisting of a word $w \in X^*$ and a polynomial $f \in K\langle X \rangle$. The left-hand side w is called *the principal part* of rule ρ. We will denote $w = \bar{\rho}$.

Let $\mathfrak{R}$ be a collection of rules on $K\langle X \rangle$. For a rule $\rho = (w, f) \in \mathscr{R}$ and a pair of words $u, v \in X^*$ consider the K-linear endomorphism $r_{u\rho v}$: $K\langle X \rangle \to K\langle X \rangle$, which fixes all words in X^* except for uwv, and sends the latter to ufv.

A rule $\rho = (w, f)$ is said to be *applicable* to a word $v \in X^*$ if w is a subword of v, i.e., $v = v'wv''$. The result of application of ρ to v is, naturally, $r_{v'\rho v''}(v) = v'fv''$. If $p \in K\langle X \rangle$ is a polynomial which involves a word v, such that a rule ρ is applicable to v, then we say that ρ is applicable to p.

A polynomial $p \in K\langle X \rangle$ is called *terminal* if no rule from $\mathscr{R}$ is applicable to v; that is, no term of p is of the form $u\bar{\rho}v$ for $\rho \in \mathscr{R}$.

Define a binary relation "$\to$" on $K\langle X \rangle$ in the following way: Set $p \to q$ if and only if there is a finite sequence of rules $\rho_1, \dots, \rho_n \in \mathscr{R}$, and a pair of sequences of words $u_i, v_i \in X^*$ such that $q = r_{u_n\rho_n v_n} \cdots r_{u_1\rho_1 v_1}(p)$.

DEFINITION 3.1. (a) A set of rules $\mathscr{R}$ is a *rewriting system* on $K\langle X \rangle$ if there are no infinite sequences of the form

$$p_1 \to p_2 \to \cdots;$$

i.e., any polynomial $p \in K\langle X \rangle$ can be modified only finitely many times by rules from $\mathscr{R}$.

(b) A rewriting system is *confluent* if for any polynomial $p \in K\langle X \rangle$ there is the unique terminal polynomial t such that $p \to t$.

Any rule $\rho = (w, f) \in \mathscr{R}$ gives rise to an identity $w - f \in K\langle X \rangle$. Let $I(\mathscr{R}) \subset K\langle X \rangle$ be the two-sided ideal generated by all such identities.

Let $v_1, v_2 \in X^*$ be a pair of words. A word $w \in X^*$ is called a *composition* of v_1 and v_2 if $w = w'uw''$, $v_1 = w'u$, $v_2 = uw''$, and $u \neq 0$.

Finally, take a word $v \in X^*$. Let us call it an ambiguity if there are two rules $\rho, \sigma \in \mathscr{R}$ such that either v is a composition of $\bar{\rho}$ and $\bar{\sigma}$ or if $v = \bar{\rho}$ and $\bar{\sigma}$ is a subword of ρ.

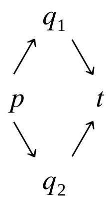
Now we can state the lemma.

LEMMA 3.2 (Diamond Lemma). (a) *A rewriting system $\mathscr{R}$ is confluent if and only if all terminal monomials form a basis of $K\langle X \rangle / I(\mathscr{R})$.*

(b) *A rewriting system is confluent if and only if it is confluent on all the ambiguities; that is, for any ambiguity $v \in X^*$ there is the unique terminal $t \in K\langle X \rangle$ such that $v \to t$.*

Remark. Statement (a) appears in [21]. A variant of Lemma 3.2 appears in [3, 4]. It was also known to Shirshov (see [25]). The name "diamond" is due to the following graphical description of the confluency property; see [21]. Let $\mathscr{R}$ be a rewriting system in the sense of Definition 3.1(a), and let "$\to$" be defined as above. Assume $p, q_1, q_2 \in K\langle X \rangle$ are such that $p \to q_1$ and $p \to q_2$. Then there is some $t \in K\langle X \rangle$ such that $q_1 \to t$ and

$q_2 \to t$:



Bergman in [2] uses the existence of a semigroup order with descending chain condition on the set of words X^*. Though in our case there is an order on the set (3.1), this order does not satisfy the descending chain condition, so we slightly modify the argument in [2].

Proof of Lemma 3.2. (a) Assume that the rewriting system $\mathscr{R}$ is confluent. Define a map r: $K\langle X\rangle \to K\langle X\rangle$ by taking $r(p)$ to be the unique terminal monomial such that $p \to r(p)$. The crucial observation is that r is a K-linear endomorphism of $K\langle X\rangle$. So if $p = \sum_i \xi_i u_i(w_i - f_i)v_i \in I(\mathscr{R})$, $\xi_i \in K$, $u_i, v_i \in X^*$, $(w_i, f_i) \in \mathscr{R}$, then $r(p) = \sum_i \xi_i r(u_i(w_i - f_i)v_i) = 0$; therefore the terminal monomials are linearly independent modulo $I(\mathscr{R})$.

Form the other side, if $\mathscr{R}$ is not confluent, then there are a polynomial $p \in K\langle X\rangle$ and terminals $q_1, q_2 \in K\langle X\rangle$ such that $p \to q_1$, $p \to q_2$, and $q_1 \neq q_2$, and then $q_1 - q_2 \in I(\mathscr{R})$.

(b) Take a polynomial $p \in K\langle X\rangle$. We prove that there is the unique terminal t such that $p \to t$ by induction on the number $n(p) = \#\{q \mid p \to q\}$. Condition (a) of Definition 3.1 assures that $n(p)$ is always finite.

If $n(p) = 0$ then p is a terminal itself and there is nothing to prove. By induction, without loss of generality we can assume that there are at least two different rules $\rho, \sigma \in \mathscr{R}$ which are applicable to p. This means that there are some words $u, v, x, y \in X^*$ such that $r_{u\rho v}(p) \neq p$, $r_{x\sigma y}(p) \neq p$, and $r_{u\rho v}(p) \neq r_{x\sigma y}(p)$. By induction, both $r_{u\rho v}(p)$ and $r_{x\sigma y}(p)$ are uniquely reduced to terminals, say, $r_{u\rho v}(p) \to t_1$ and $r_{x\sigma y}(p) \to t_2$. We need to show that $t_1 = t_2$.

Consider two cases: when $\bar{\rho}$ and $\bar{\sigma}$ have common symbols in p, and thus $u\bar{\rho}v = x\bar{\sigma}y$ is a word in p; and when $\bar{\rho}$ and $\bar{\sigma}$ are disjoint.

In the first case, let $w \in X^*$ be the union of $\bar{\rho}$ and $\bar{\sigma}$ in p. Then w is an ambiguity. By assumption, there is the unique terminal $s \in K\langle X\rangle$ such that $w \to s$. Let $q \in K\langle X\rangle$ be obtained from p by substituting w by s.

Then we have

$$\begin{array}{ccc} & r_{u\bar{\rho}v}(p) & \\ \nearrow & & \searrow \\ p & & q \\ \searrow & & \nearrow \\ & r_{x\bar{\sigma}y}(p) & \end{array} \tag{3.4}$$

By induction, q is uniquely reduced to a terminal t, and therefore one has $r_{u\rho v}(p) \to t$ and $r_{x\sigma y}(p) \to t$.

In the second case, note that $r_{x\sigma y} r_{u\rho v}(p) = r_{u\rho v} r_{x\sigma y}(p)$. Denote this polynomial by q. Then relations (3.4) still hold, and we finish by the same argument as in the first case. ∎

3.4. *Basis of a Free Vertex Algebra*

Return to the setup of Section 3.1. From now on we take the locality function $N(a,b)$ to be constant: $N(a,b) \equiv N$. Let $C = C(N)$ be the free Lie conformal algebra and let $L = \operatorname{Coeff} C$ be its Lie algebra of coefficients; see Proposition 3.1. In this section we build a basis of the universal enveloping algebra $U(L)$ of L and a basis of the free vertex algebra $V = V(C)$.

We start by endowing $\mathscr{B}$ with an arbitrary linear order. Then we define a linear order on the set X of generators of L, given by (3.1), in the following way:

$$a(m) < b(n) \Leftrightarrow m < n \text{ or } (m = n \text{ and } a < b). \tag{3.5}$$

On the set X^* of words in X introduce the standard lexicographical order: For $u, v \in X^*$ if $|u| < |v|$, set $u < v$; if $|u| = |v|$, then set $u < v$ whenever there is some $1 \le i \le |v|$ such that $u(i) < v(i)$ and $u(j) = v(j)$ for all $1 \le j < i$.

In a defining relation from (3.2) the biggest term has form $b(n)a(m)$ such that

$$n - m > N \text{ or } \big(n - m = N \text{ and } \big(b > a \text{ or } (b = a \text{ and } N \text{ is odd})\big)\big). \tag{3.6}$$

Taking it as a principal part, we get a rule on $\Bbbk\langle X\rangle$

$$\rho(b(n), a(m)) = \left(b(n)a(m), a(m)b(n) - \sum_{s=1}^{N} (-1)^s \binom{N}{s} [b(n-s), a(m+s)] \right), \tag{3.7a}$$

and in the case when $a = b$, $n - m = N$, and N is odd,

$$\rho(a(m+N), a(m)) = \Bigg(a(m+N)a(m), a(m)a(m+N) - \frac{1}{2} \sum_{s=1}^{(N-1)/2} (-1)^s \binom{N}{s} [a(n-s), a(m+s)] \Bigg). \quad (3.7b)$$

Denote the set of all such rules by $\mathscr{R}$:

$$\mathscr{R} = \{\rho(b(n), a(m)) \,|\, (3.6) \text{ holds}\}. \quad (3.8)$$

LEMMA 3.3. *The set of rules $\mathscr{R}$ is a confluent rewriting system on $\Bbbk\langle X\rangle$.*

We prove this lemma in Section 3.5. Here we derive from it and from Lemma 3.2 the following theorem.

THEOREM 3.1. (a) *Let $C = C(N)$ be the free Lie conformal algebra generated by a linearly ordered set $\mathscr{B}$ corresponding to a constant locality function N. Let $L = \operatorname{Coeff} C$ be the Lie algebra of coefficients and let $U = U(L)$ be its universal enveloping algebra. Then a basis of U is given by all monomials*

$$a_1(n_1)a_2(n_2)\cdots a_k(n_k), \qquad a_i \in \mathscr{B}, n_i \in \mathbb{Z}, \quad (3.9)$$

such that for any $1 \le i < k$ one has

$$n_i - n_{i+1} \le \begin{cases} N-1 & \text{if } a_i > a_{i+1} \text{ or } (a_i = a_{i+1} \text{ and } N \text{ is odd}), \\ N & \text{otherwise}. \end{cases} \quad (3.10)$$

(b) *A basis of the algebra $U(L_+)$ is given by all monomials* (3.9) *satisfying the condition* (3.10) *and such that all $n_i \ge 0$.*

(c) *Let $V = V(C)$ be the corresponding free vertex algebra. Then a basis of V consists of elements*

$$a_1(n_1)a_2(n_2)\cdots a_k(n_k k)\mathbb{1}, \qquad a_i \in \mathscr{B}, n_i \in \mathbb{Z}, \quad (3.11)$$

such that the condition (3.10) *holds and, in addition, $n_k < 0$.*

Proof. Statement (a) is a direct corollary of Lemmas 3.3 and 3.2, because (3.9) is precisely the set of all terminal monomials with respect to $\mathscr{R}$.

Statement (b) follows immediately from Lemma 3.1, since any subset of rules $\mathscr{R}$ is also a confluent rewriting system. Note also that for a rule ρ given by (3.7) if the principal term $\bar{\rho}$ contains only elements from X_0 then so does the whole rule ρ.

For the proof of (c) recall that $V \cong U/UL_+$ as linear spaces (and even as L-modules), where UL_+ is the left ideal generated by L_+; see Section 2.4. By Lemma 3.1, this ideal is the linear span of all monomials $a_1(n_1)a_2(n_2)\cdots a_k(n_k)$ such that $n_k \geq 0$. But under the action of the rewriting system $\mathscr{R}$ the index of the rightmost symbol in a word can only increase; hence the linear span of these monomials in $\Bbbk\langle X\rangle$ is stable under $\mathscr{R}$. It follows that the terminal monomials with a non-negative rightmost index form a basis of UL_+. This proves (b). ∎

3.5. *Proof of Lemma* 3.3

First we prove that the set of rules $\mathscr{R}$, given by (3.8), is a rewriting system on $\Bbbk\langle X\rangle$. Take a word $u = a_1(m_1)\cdots a_k(m_k) \in X^*$. Let $p \in \Bbbk\langle X\rangle$ be such that $u \to p$. Then any word v that appears in p lies in the finite set

$$W_u = \left\{ b_1(n_1)\cdots b_k(n_k) \in X^* \middle| n_i \geq \min_{1\leq j\leq k}\{m_j\} \text{ and } \sum n_i = \sum m_i \right\}. \tag{3.12}$$

Therefore condition (a) of Definition 3.1 holds.

Thus we are left to prove that $\mathscr{R}$ is confluent. According to Lemma 3.2, it is enough to check that it is confluent on a composition $w = c(k)b(j)a(i)$ of principal parts of a pair of rules $\rho(b(j), a(i)), \rho(c(k), b(j)) \in \mathscr{R}$. Thus it is sufficient to prove the following claim.

LEMMA 3.4. *Let $u = c(k)b(j)a(i) \in X^*$ be a word of length* 3. *Then $\mathscr{R}$ is confluent on u; i.e., there is a unique terminal $r(w) \in \Bbbk\langle X\rangle$ such that $u \to r(w)$.*

Proof. Assume for simplicity that the three rules $\rho(b(n), a(m))$, $\rho(c(p), b(n))$, and $\rho(c(p), a(m))$ are of the form (3.7a). The general case is essentially the same, but requires some additional calculations.

Consider the set W_u, given by (3.12). We prove that the lemma holds for all $w \in W_u$ by induction on w. If w is sufficiently small then it is a terminal itself. By induction, it is enough to consider $w = c(p)b(n)a(m) \in W_u$ such that $\mathscr{R}$ is applicable to both $b(n)a(m)$ and $c(p)b(n)$. Apply

$\rho(b(n), a(m))$ and $\rho(c(p), b(n))$ to w and take the difference of the results:

$$v = b(n)c(p)a(m) - \sum_{s=1}^{N} (-1)^s \binom{N}{s} [c(p-s), b(n+s)] a(m)$$
$$- c(p)a(m)b(n) + \sum_{s=1}^{N} (-1)^s \binom{N}{s} c(p) [b(n-s), a(m+s)].$$

By induction, v is reduced uniquely to a terminal t and we only have to show that $t = 0$. First we apply the rules $\rho(b(n), a(m))$, $\rho(c(p), b(n))$, and $\rho(c(p), a(m))$ to v several times and get

$$\begin{aligned} v \to & - \sum_{s=1}^{N} (-1)^s \binom{N}{s} b(n) [c(p-s), a(m+s)] + b(n)a(m)c(p) \\ & + \sum_{s=1}^{N} (-1)^s \binom{N}{s} [c(p-s), a(m+s)] b(n) - a(m)c(p)b(n) \\ & - \sum_{s=1}^{N} (-1)^s \binom{N}{s} [c(p-s), b(n+s)] a(m) \\ & + \sum_{s=1}^{N} (-1)^s \binom{N}{s} c(p) [b(n-s), a(m+s)] \\ & \to \sum_{s=1}^{N} (-1)^s \binom{N}{s} [a(m), [c(p-s), b(n+s)]] \\ & + \sum_{s=1}^{N} (-1)^s \binom{N}{s} [[c(p-s), a(m+s)], b(n)] \\ & + \sum_{s=1}^{N} (-1)^s \binom{N}{s} [c(p), [b(n-s), a(m+s)]]. \end{aligned} \tag{3.13}$$

Next we introduce two rules acting on the linear combinations of (formal) commutators: For any $a(m), b(n), c(p) \in X$ let

$$\kappa = \big([a(m), [b(n), c(p)]], [[a(m), b(n)], c(p)] + [b(n), [a(m), c(p)]]\big),$$

$$\lambda = \left([b(n), a(m)], -\sum_{s=1}^{N} (-1)^s \binom{N}{s} [b(n-s), a(m+s)]\right).$$

The rule λ is the locality relation, and κ is nothing else but the Jacoby identity. The lemma will be proved after we show two things:

(1) *There always exists a finite sequence of applications of the rules* κ *and* λ *that reduces* (3.13) *to* 0.

(2) *All words which appear in the process of reduction in* (1) *are smaller than the initial word* $u = c(p)b(n)a(m)$ *with respect to the order* (3.5).

Indeed, assume (1) and (2) hold. Denote the polynomial in (3.13) by p_0. Let

$$p_0 \to p_1 \to \cdots \to 0$$

be the reduction, guaranteed by (1). By (2) and by the induction hypothesis, any two neighboring polynomials $p_i \to p_{i+1}$ from this sequence are uniquely $\mathscr{R}$-reduced to a terminal, and this terminal must be the same, since either $p_i \overset{\mathscr{R}}{\to} p_{i+1}$ or $p_{i+1} \overset{\mathscr{R}}{\to} p_i$.

Denote the three last terms in (3.13) by $\boxed{\text{a}}$, $\boxed{\text{b}}$, and $\boxed{\text{c}}$. In Fig. 1 we present a scheme of how κ and λ should be applied in order to reduce (3.13) to 0.

Each box in Fig. 1 stands for a sum of commutators:

$$\boxed{\text{j}} = -\boxed{\text{r}}$$
$$= \sum_{s,t=1}^{N} (-1)^{s+t} \binom{N}{s} \binom{N}{t} [[c(p-s-t), a(m+t)], b(n+s)],$$

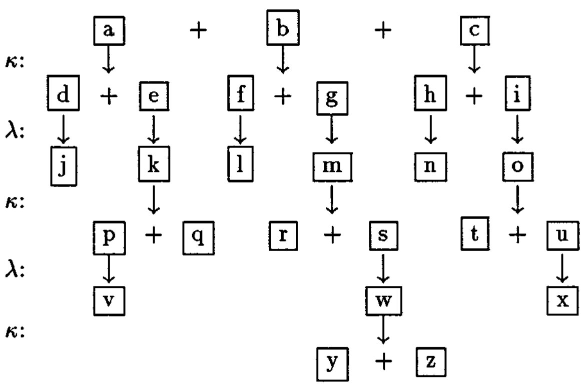


FIG. 1. Application of rules κ and λ.

$$\boxed{\text{k}} = \sum_{s,t=1}^{N} (-1)^{s+t} \binom{N}{s} \binom{N}{t} [c(p-s), [b(n+s-t), a(m+t)]],$$

$$\boxed{\text{l}} = -\boxed{\text{t}} = \sum_{s,t=1}^{N} (-1)^{s+t} \binom{N}{s} \binom{N}{t}$$
$$\times [c(p-s), [b(n-t), a(m+s+t)]],$$

$$\boxed{\text{m}} = \sum_{s,t=1}^{N} (-1)^{s+t} \binom{N}{s} \binom{N}{t} [[b(n+t), c(p-s-t)], a(m+s)],$$

$$\boxed{\text{n}} = -\boxed{\text{q}} = \sum_{s,t=1}^{N} (-1)^{s+t} \binom{N}{s} \binom{N}{t}$$
$$\times [[b(n-s+t), c(p-t)], a(m+s)],$$

$$\boxed{\text{o}} = \sum_{s,t=1}^{N} (-1)^{s+t} \binom{N}{s} \binom{N}{t} [b(n-s), [a(m+s+t), c(p-t)]],$$

$$\boxed{\text{v}} = -\boxed{\text{y}} = \sum_{s,t,r=1}^{N} (-1)^{s+t+r} \binom{N}{s} \binom{N}{t} \binom{N}{r}$$
$$[b(n+s-t), [a(m+t+r), c(p-s-r)]],$$

$$\boxed{\text{w}} = \sum_{s,t,r=1}^{N} (-1)^{s+t+r} \binom{N}{s} \binom{N}{t} \binom{N}{r}$$
$$\times [[a(m+s+r), b(n+t-r)], c(p-s-t)],$$

$$\boxed{\text{x}} = -\boxed{\text{z}} = \sum_{s,t,r=1}^{N} (-1)^{s+t+r} \binom{N}{s} \binom{N}{t} \binom{N}{r}$$
$$\times [a(m+s+t), [c(p-t-r), b(n-s+r)]].$$

One can see that all terminal boxes in the above scheme cancel, so that $\boxed{\text{a}} + \boxed{\text{b}} + \boxed{\text{c}} \to 0$. Claim (2) also holds, since every symbol in every box in Fig. 1 is less than $c(p)$. ∎

3.6. *Digression on Hall Bases*

Let again $\mathscr{B}$ be some linearly ordered alphabet, $N \in \mathbb{Z}_+$, $C = C(N)$ the free Lie conformal algebra generated by $\mathscr{B}$ with respect to the constant locality N, and $L = \operatorname{Coeff} C(N)$. A basis of the Lie algebra L could be obtained by modifying the construction of a Hall basis of a free Lie algebra; see [12, 23, 24]. Here we review the latter construction. We closely follow [22], except that all the order relations are reversed.

As in Section 3.3, take an alphabet X and a commutative ring K. Let $T(X)$ be the set of all binary trees with leaves from X. For typographical reasons we will write the tree $\widehat{xy}$ as $\langle x, y\rangle$. Assume that $T(X)$ is endowed with a linear order such that $\langle x, y\rangle > \min\{x, y\}$ for any $x, y \in T(X)$.

DEFINITION 3.2. A *Hall set* $\mathscr{H} \subset T(X)$ is a subset of all trees $h \in T(X)$ satisfying the following (recursive) properties:

1. If $h = \langle x, y\rangle$ then $y, x \in \mathscr{H}$ and $x > y$.
2 If $h = \langle\langle x, y\rangle, z\rangle$ then $z \geq y$, so that $\langle x, y\rangle > z \geq y$.

In particular, $X \subset \mathscr{H}$.

Introduce two maps α: $T(X) \to X^*$ and λ: $T(X) \to K\langle X\rangle$ in the following recursive way: For $a \in X$ set $\alpha(a) = \lambda(a) = a$ and $\alpha(\langle x, y\rangle) = \alpha(x)\alpha(y)$, $\lambda(\langle x, y\rangle) = [\lambda(x), \lambda(y)]$.

It is a well-known fact (see, e.g., [22]) that

(a) *$\lambda(\mathscr{H})$ is a basis of the free Lie algebra generated by X and*

(b) *$\alpha|_{\mathscr{H}}$ is injective.*

A word $w \in \alpha(\mathscr{H})$ is called a *Hall word*.

On the set X^* of words in X introduce a (lexicographic) order as follows: If u is a prefix of v then $u > v$; otherwise $u > v$ whenever for some index i one has $u_i > v_i$ and $u_j = v_j$ for all $j < i$.

DEFINITION 3.3 [25, 7]. A word $v \in X^*$ is called *Lyndon–Shirshov* if it is bigger than all its proper suffices.

PROPOSITION 3.2. (a) *There is a Hall set $\mathscr{H}_{\mathrm{LS}}$ such that $\alpha(\mathscr{H}_{\mathrm{LS}})$ is the set of all Lyndon–Shirshov words and α: $T(X) \to X^*$ preserves the order.*

(b) *For any tree $h \in \mathscr{H}_{\mathrm{LS}}$ the biggest term in $\lambda(h)$ is $\alpha(h)$.*

3.7. *Basis of the Algebra of Coefficients of a Free Lie Conformal Algebra*

Here we apply general results from Section 3.6 to the situation of Section 3.1.

Recall that starting from a set of symbols $\mathscr{B}$ and a number $N > 0$, we build the free conformal algebra $C = C(N)$ generated by $\mathscr{B}$ such that $a \textcircled{n} b = 0$ for any two $a, b \in \mathscr{B}$ and $n \geq N$. Let $L = \operatorname{Coeff} C$ be the corresponding Lie algebra of coefficients. It is generated by the set $X = \{a(n) \mid a \in \mathscr{B}, n \in \mathbb{Z}\}$ subject to relations (3.2).

The set of generators X is equipped with the linear order defined by (3.5). W define the order on X^* as in Section 3.6. Consider the set of all Lyndon words in X^* and let $\mathscr{H} = \mathscr{H}_{\mathrm{LS}} \subset T(X)$ be the corresponding Hall set. Recall that there is a rewriting system $\mathscr{R}$ on $\Bbbk\langle X\rangle$, given by (3.8). Define

$$\mathscr{H}_{\text{term}} = \{h \in \mathscr{H} \mid \alpha(h) \text{ is terminal}\}.$$

LEMMA 3.5. (a) *Let $v_1 \leq \cdots \leq v_n$ be a non-decreasing sequence of terminal Lyndon–Shirshov words. Then their concatenation $w = v_1 \cdots v_n \in X^*$ is a terminal word.*

(b) *Each terminal word $w \in X^*$ can be uniquely represented as a concatenation $w = v_1 \cdots v_n$, where $v_1 \leq \cdots \leq v_n$ is a non-decreasing sequence of terminal Lyndon–Shirshov words.*

Proof. (a) Take two terminal Lyndon–Shirshov words $v_1 \leq v_2$. Let $x \in X$ be the last symbol of v_1 and let $y \in X$ be the first symbol of v_2. Then, since a word is less than its prefix and since v_1 is a Lyndon–Shirshov word, we get

$$x < v_1 \leq v_2 < y.$$

Therefore, xy is a terminal, and hence $v_1 v_2$ is a terminal, too.

(b) Take a terminal word $w \in X^*$. Assume it is not Lyndon–Shirshov. Let v be the maximal among all proper suffices of w. Then v is Lyndon–Shirshov, $v > w$, and $w = uv$ for some word u. By induction, $u = v_1 \cdots v_{n-1}$ for a non-decreasing sequence of Lyndon–Shirshov words $v_1 \leq \cdots \leq v_{n-1}$. We are left to show that $v \geq v_{n-1}$.

Assume on the contrary that $v < v_{n-1}$. Then, since $v > v_{n-1}v$, v_{n-1} must be a prefix of v so that $v = v_{n-1}v'$. But then $v' > v$ which contradicts the Lyndon–Shirshov property of v.

The uniqueness is obvious. ∎

Let φ: $\Bbbk\langle X\rangle \to U(L)$ be the canonical projection with the kernel $I(\mathscr{R})$.

THEOREM 3.2. *The set $\varphi(\lambda(\mathscr{H}_{\text{term}}))$ is a basis of L.*

Proof. Let $s = \{h_1, \dots, h_n\} \subset \mathscr{H}_{\text{term}}$ be a non-decreasing sequence of terminal Hall trees. Let $\lambda(s) = \lambda(h_1) \cdots \lambda(h_n) \in \Bbbk\langle X\rangle$ and $\alpha(s) = \alpha(h_1) \cdots \alpha(h_n) \in X^*$.

By the Poincaré–Birkhoff–Witt theorem it is sufficient to prove that the set $\{\varphi(\lambda(s))\}$, when s ranges over all non-decreasing sequences s of terminal Hall trees, is a basis of $U(L)$.

By Proposition 3.2 (b), $\lambda(s) = \alpha(s) + O(\alpha(s))$, where $O(v)$ stands for a sum of terms which are less than v. Now let $t(s) \in \Bbbk\langle X\rangle$ be a terminal such that $\lambda(s) \to t(s)$. One can view $t(s)$ as the decomposition of $\varphi(\lambda(s))$ in basis (3.9). By Lemma 3.5, $\alpha(s)$ is a terminal monomial; hence $t(s)$ has form $t(s) = \alpha(s) + f(s)$ where $f(s)$ is a sum of terms $v \in X^*$ satisfying the following properties:

1. v is terminal and $v < \alpha(s)$.

2. If v contains a symbol $a(n) \in X$ then a appears in $\alpha(s)$ and $n_{\min} \leq n \leq n_{\max}$, where $n_{\min}$ and $n_{\max}$ are, respectively, minimum and maximum of all indices that appear in $\alpha(s)$.

Indeed, due to Proposition 3.2(b) properties 1 and 2 are satisfied by all the terms in $\lambda(s) - \alpha(s)$, and they cannot be broken by an application of the rules $\mathscr{R}$.

Property 1 implies that all $t(s)$ and, therefore, $\varphi(\lambda(s))$ are linearly independent. So we are left to show that they span $U(L)$. For that purpose we show that any terminal word $w \in X^*$ can be represented as a linear combination of $t(s)$.

By Lemma 3.5(b) any terminal word w could be written as $w = \alpha(s)$ for some non-decreasing sequence s of terminal Hall trees. So we can write $w = t(s) - f(s)$. Now do the same with any term v that appears in $f(s)$, and so on. This process should terminate, because every term v that appears during this process must satisfy properties 1 and 2 and there are only finitely many such terms. ∎

Remark. Alternatively we could use the theorem of Bokut' and Malcolmson [5].

As in Theorem 3.1(b), we deduce that all the elements of $\varphi(\lambda(\mathscr{H}_{\text{term}}))$ containing only symbols from X_0 form a basis of L_+.

Note that we have an algorithm for building a basis of the free Lie conformal algebra $C = C(N)$. Let $L = \operatorname{Coeff} C$, $V = V(C)$, and $U = U(L)$. Recall that the image if C in V under the canonical embedding $\psi: C \to V$ is $\psi(C) = L_- \mathbb{1} = L\mathbb{1} \subset V$. So, the algorithm goes as follows: Take the basis of L provided by Theorem 3.2. Decompose its element in basis (3.9) of the universal enveloping algebra $U(L)$, and then cancel all terms of the form $a_1(n_1) \cdots a_k(n_k)$ where $n_k \geq 0$. What remains, being interpreted as elements of the vertex algebra V, form a basis of $\psi(C) \subset V$.

3.8. *Basis of the Algebra of Coefficients of a Free Associative Conformal Algebra*

Let again $\mathscr{B}$ be some alphabet, and let $N: \mathscr{B} \times \mathscr{B} \to \mathbb{Z}_+$ be a locality function, not necessarily constant and not necessarily symmetric. By Proposition 3.1, the coefficient algebra $A = \operatorname{Coeff} C(N)$ of the free associative conformal algebra $C(N)$ corresponding to the locality function N is presented in terms of generators and relations by the set of generators $X = \{b(n) \mid b \in \mathscr{B}, n \in \mathbb{Z}\}$ and relations (3.2).

THEOREM 3.3. (a) *A basis of the algebra A is given by all monomials of the form*

$$a_1(n_1)\cdots a_{l-1}(n_{l-1})a_l(n_l), \tag{3.14}$$

where $a_i \in \mathscr{B}$ and

$$-\left\lceil \frac{N_i - 1}{2} \right\rceil \le n_i \le \left\lfloor \frac{N_i - 1}{2} \right\rfloor,$$
$$N_i = N(a_i, a_{i+1}) \qquad \text{for } i = 1, \ldots, l-1.$$

(b) *A basis of the algebra A_+ is given by all monomials of the form*

$$a_1(n_1)\cdots a_{l-1}(n_{l-1})a_l(n_l), \tag{3.15}$$

where $a_i \in \mathscr{B}$ and

$$0 \le n_i \le N_i - 1, \qquad N_i = N(a_i, a_{i+1}) \qquad \text{for } i = 1, \ldots, l-1.$$

COROLLARY 3.1. *Assume that the locality function N is constant. Consider the homogeneous component $A_{k,l}$ of A, spanned by all the words of length l and of the sum of indexes k. Then* $\dim A_{k,l} = N^{l-1}$.

Proof of Theorem 3.3. (a) Introduce a linear order on $\mathscr{B}$ and define an order on the set of generators X by the rule

$$a(m) > b(n) \Leftrightarrow |m| > |n| \text{ or } m = -n > 0 \text{ or } (m = n \text{ and } a > b).$$

In particular, for some $a \in \mathscr{B}$ we have

$$a(0) < a(-1) < a(1) < a(-2) < a(2) < \cdots .$$

For any relation r from (3.2) take the biggest term $\bar{r}$ and consider the rule $(\bar{r}, r - \bar{r})$. This way we get a collection of rules

$$\mathscr{R} = \left\{ \rho_1(b(n), a(m)) \,\middle|\, a, b \in \mathscr{B},\, n > \left\lfloor \frac{N(b,a) - 1}{2} \right\rfloor \right\}$$
$$\cup \left\{ \rho_2(b(n), a(m)) \,\middle|\, n < -\left\lceil \frac{N(b,a) - 1}{2} \right\rceil \right\},$$

where

$$\rho_1(b(n), a(m)) = \left(b(n)a(m), \sum_{s=1}^{N(b,a)} (-1)^{s+1} \binom{N(b,a)}{s} b(n-s)a(m+s) \right),$$

$$\rho_2(b(n), a(m)) = \left(b(n)a(m), \sum_{s=1}^{N(b,a)} (-1)^{s+1} \binom{N(b,a)}{s} b(n+s)a(m-s) \right).$$

By Lemma 3.2, we have to prove that these rules form a confluent rewriting system on $\Bbbk\langle X \rangle$. Clearly $\mathscr{R}$ is a rewriting system, since it decreases the order, and each subset of $\Bbbk\langle X \rangle$, containing only finitely many different letters from $\mathscr{B}$, has the minimal element, in contrast to the situation of Section 3.5.

As before, it is enough to check that $\mathscr{R}$ is confluent on any composition $w = c(p)b(n)a(m)$, of the principal parts of rules from $\mathscr{R}$. Consider the set $W = \{c(k)b(j)a(i) \mid k, j, i \in \mathbb{Z}\} \subset X^*$. We prove by induction on $w \in W$ that $\mathscr{R}$ is confluent on w. If w is sufficiently small, then it is terminal. Assume that $w = c(k)b(j)a(i)$ is an ambiguity, for example, that $\rho_1(c(p), b(n))$ and $\rho_2(b(n), a(m))$ are both applicable to w. Other cases are done in the same way. Let

$$w_1 = \rho_1(c(p), b(n))(w) = \sum_{s=1}^{N(c,b)} (-1)^s \binom{N(c,b)}{s} c(p-s)b(n+s)a(m),$$

$$w_2 = \rho_2(b(n), a(m))(w) = \sum_{t=1}^{N(b,a)} (-1)^t \binom{N(b,a)}{t} c(p)b(n+t)a(m-t).$$

Applying $\rho_2(b(n+s), a(m))$ for $s = 1, \ldots, N(b,a)$ to w_1 gives the same result as we get from applying $\rho_1(c(p), b(n+t))$ for $t = 1, \ldots, N(c,b)$ to w_2, namely,

$$\sum_{s,t \geq 1} (-1)^{s+t} \binom{N(c,b)}{s} \binom{N(b,a)}{t} c(p-s)b(n+s+t)a(m-t). \tag{3.16}$$

By the induction assumption, $w_1 - w_2$ is uniquely reduced to a terminal, and since all monomials in (3.16) are smaller than w, we conclude that this terminal must be 0.

(b) Follows at once from Lemma 3.1. ∎

ACKNOWLEDGMENTS

I am grateful to Bong Lian, Efim Zelmanov, and Gregg Zuckerman for helpful discussions. I thank Victor Kac, Bong Lian, and Gregg Zuckerman for communicating unpublished papers [17, 16, 20] and I thank L. A. Bokut' who carefully read this paper and made valuable comments.

REFERENCES

1. A. A. Belavin, A. M. Polyakov, and A. B. Zamolodchikov, Infinite conformal symmetry in two-dimensional quantum field theory, *Nuclear Phys. B* **241**, No. 2 (1984), 333–380.
2. G. M. Bergman, The diamond lemma for ring theory, *Adv. in Math.* **29**, No. 2 (1978), 178–218.
3. L. A. Bokut', Unsolvability of the word problem, and subalgebras of finitely presented Lie algebras, *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 1173–1219.
4. L. A. Bokut', Imbeddings into simple associative algebras, *Algebra i Logika* **15**, No. 2 (1976), 117–142, 245.
5. L. A. Bokut' and P. Malcolmson, Gröbner–Shirshov bases for relations of a Lie algebra and its enveloping algebra, preprint.
6. R. E. Borcherds, Vertex algebras, Kac–Moody algebras, and the Monster, *Proc. Nat. Acad. Sci. U.S.A.* **83**, No. 10 (1986), 3068–3071.
7. K.-T. Chen, R. H. Fox, and R. C. Lyndon, Free differential calculus IV. The quotient groups of the lower central series, *Ann. of Math.* (*2*) **68** (1958), 81–95.
8. P. M. Cohn, "Universal Algebra," Mathematics and Its Applications, Vol. 6, 2nd ed., Dordrecht, 1981.
9. I. B. Frenkel, Y.-Z. Huang, and J. Lepowsky, On axiomatic approaches to vertex operator algebras and modules, *Mem. Amer. Math. Soc.* **104**, No. 494 (1993).
10. I. B. Frenkel, J. Lepowsky, and A. Merman, "Vertex Operator Algebras and the Monster," Academic Press, Boston, 1988.
11. I. B. Frenkel and Y. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, *Duke Math. J.* **66**, No. 1 (1992), 123–168.
12. M. Hall, Jr., A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.* **1** (1950), 575–581.
13. N. Jacobson, "Basic Algebra II," 2nd ed., Freeman, New York, 1989.
14. V. G. Kac, "Infinite-Dimensional Lie Algebras," 3rd ed., Cambridge Univ. Press, Cambridge, UK, 1990.
15. V. G. Kac, "Vertex Algebras for Beginners," University Lecture Series, Vol. 10, Amer. Math. Soc., Providence, 1996.
16. V. G. Kac, Formal distribution algebras and conformal algebras, a talk at the Brisbane Congress on Mathematical Physics, July 1997.

17. V. G. Kac, The idea of locality, *in* "Physical Applications and Mathematical Aspects of Geometry, Groups and Algebras (H.-D. Doebner *et al.*, Eds.), pp. 16–32, World Scientific, Singapore, 1997.
18. B. H. Lian and G. J. Zuckerman, Commutative quantum operator algebras, *J. Pure Appl. Algebra* **100**, No. 1–3 (1995), 117–139.
19. B. H. Lian and G. J. Zuckerman, Moonshine cohomology, *Sūrikaisekikenkyūsho Kōkyūroku* No. 904 (1995), 87–115; Moonshine and vertex operator algebra (Japanese) (Kyoto, 1994).
20. B. H. Lian and G. J. Zuckerman, preprint.
21. M. H. A. Newman, On theories with a combinatorial definition of "equivalence," *Ann. of Math.* (*2*) **43** (1942), 223–243.
22. C. Reutenauer, "Free Lie Algebras," London Mathematical Society Monographs, New Series, Vol. 7, Clarendon Press/Oxford Univ. Press, New York, 1993.
23. A. I. Shirshov, On free Lie rings, *Mat. Sb. N.S.* **45**, No. 87 (1958), 113–122.
24. A. I. Shirshov, Bases of free Lie algebras, *Algebra i Logika* **1** (1962), 14–19.
25. A. I. Shirshov, Some algorithm problems for Lie algebras, *Sibirsk. Mat. Zh.* **3** (1962), 292–296.