

Some elements of the hyperalgebra of $\mathrm{SL}(2, k)$ in positive characteristic and their applications

Yutaka Yoshii

College of Education, Ibaraki University

1 Introduction

In the study of the representation theory of a finite-dimensional algebra R over a field, it is meaningful to decompose the identity element of R into a sum of pairwise orthogonal primitive idempotents. Indeed, if such a decomposition can be given explicitly, a direct sum decomposition of the R -module R into projective indecomposable modules is obtained, and furthermore, all projective indecomposable R -modules can be obtained.

Now, let k be an algebraically closed field of characteristic $p > 0$ and G a simply connected and simple algebraic group defined and split over \mathbb{F}_p . For $r \in \mathbb{Z}_{>0}$, let G_r be the r -th Frobenius kernel of G . The study of the representation theory of the hyperalgebra $\mathcal{U}_r = \mathrm{Dist}(G_r)$ is indispensable for studying the representation theory of G . Since \mathcal{U}_r is a finite-dimensional k -algebra, if one can obtain the above decomposition of its identity element explicitly, then the projective indecomposable \mathcal{U}_r -modules can be constructed. However, up to the present, almost nothing is known about the decomposition in \mathcal{U}_r . Only in the simplest case, where $G = \mathrm{SL}(2, k)$ and p is an odd prime, has such a decomposition been given for \mathcal{U}_1 , as shown by Seligman [3].

The author has recently succeeded in generalizing Seligman's result to arbitrary p and r . More specifically, the author has succeeded in constructing several elements of \mathcal{U}_r for $G = \mathrm{SL}(2, k)$ (these elements are denoted by $B^{(\epsilon)}(\mathbf{a}, \mathbf{j})$), which include pairwise orthogonal primitive idempotents of \mathcal{U}_r whose sum is the identity element. Furthermore, it has been found that these elements possess various interesting properties and have several applications. In this article, we review the main results from the author's recent series of studies obtained using these elements. For details, see [5], [6], [7], and [8].

2 Preliminaries

Let

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

be the standard basis in the Lie algebra $\mathfrak{g}_{\mathbb{C}} = \mathfrak{sl}(2, \mathbb{C})$. Let $\mathcal{U}_{\mathbb{C}}$ be the universal enveloping algebra of $\mathfrak{g}_{\mathbb{C}}$. Set $X^{(n)} = X^n/n!$, $Y^{(n)} = Y^n/n!$, and $\binom{H+c}{n} = \prod_{j=1}^n (H+c-j+1)/n!$ in $\mathcal{U}_{\mathbb{C}}$ for $n \in \mathbb{Z}_{\geq 0}$ and $c \in \mathbb{Z}$. Let $\mathcal{U}_{\mathbb{Z}}$ be the subring of $\mathcal{U}_{\mathbb{C}}$ generated by all $X^{(m)}$ and

$Y^{(m)}$ with $m \geq 0$. Let $G = \text{SL}(2, k)$ be the special linear group of degree 2 over k . Let $\mathcal{U} = \mathcal{U}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k (\cong \text{Dist}(G))$ be the hyperalgebra of G . We use the same symbols for images in \mathcal{U} of the elements of $\mathcal{U}_{\mathbb{Z}}$ (for example, $X^{(m)}$, $Y^{(m)}$, $\binom{H+c}{n}$, and so on). Then we have $\mathcal{U} = \langle X^{(m)}, Y^{(m)} \mid m \geq 0 \rangle_{k\text{-alg.}}$. Moreover, we define subalgebras \mathcal{U}^+ , \mathcal{U}^- , \mathcal{U}^0 , and \mathcal{A} as

$$\begin{aligned}\mathcal{U}^+ &= \langle X^{(m)} \mid m \geq 0 \rangle_{k\text{-alg.}}, \\ \mathcal{U}^- &= \langle Y^{(m)} \mid m \geq 0 \rangle_{k\text{-alg.}}, \\ \mathcal{U}^0 &= \left\langle \binom{H}{n} \mid n \geq 0 \right\rangle_{k\text{-alg.}}, \\ \mathcal{A} &= \langle \mathcal{U}^0, Y^{(m)} X^{(m)} \mid m \geq 0 \rangle_{k\text{-alg.}}.\end{aligned}$$

For a fixed positive integer r , set

$$\begin{aligned}\mathcal{U}_r &= \langle X^{(m)}, Y^{(m)} \mid 0 \leq m \leq p^r - 1 \rangle_{k\text{-alg.}}, \\ \mathcal{U}_r^+ &= \mathcal{U}^+ \cap \mathcal{U}_r = \langle X^{(m)} \mid 0 \leq m \leq p^r - 1 \rangle_{k\text{-alg.}}, \\ \mathcal{U}_r^- &= \mathcal{U}^- \cap \mathcal{U}_r = \langle Y^{(m)} \mid 0 \leq m \leq p^r - 1 \rangle_{k\text{-alg.}}, \\ \mathcal{U}_r^0 &= \mathcal{U}^0 \cap \mathcal{U}_r = \left\langle \binom{H}{n} \mid 0 \leq n \leq p^r - 1 \right\rangle_{k\text{-alg.}}, \\ \mathcal{A}_r &= \mathcal{A} \cap \mathcal{U}_r = \langle \mathcal{U}_r^0, Y^{(m)} X^{(m)} \mid 0 \leq m \leq p^r - 1 \rangle_{k\text{-alg.}}.\end{aligned}$$

Then the multiplication maps

$$\mathcal{U}^- \otimes_k \mathcal{U}^0 \otimes_k \mathcal{U}^+ \rightarrow \mathcal{U}, \quad \mathcal{U}_r^- \otimes_k \mathcal{U}_r^0 \otimes_k \mathcal{U}_r^+ \rightarrow \mathcal{U}_r$$

are k -linear isomorphisms.

The standard k -bases and dimensions of the above algebras are summarized in the following table.

Algebra R	A k -basis of R	$\dim_k R$
\mathcal{U}	$\{Y^{(m_1)} \binom{H}{n} X^{(m_2)} \mid m_1, m_2, n \geq 0\}$	∞
\mathcal{U}^+	$\{X^{(m)} \mid m \geq 0\}$	∞
\mathcal{U}^-	$\{Y^{(m)} \mid m \geq 0\}$	∞
\mathcal{U}^0	$\{\binom{H}{n} \mid n \geq 0\}$	∞
\mathcal{A}	$\{Y^{(m)} \binom{H}{n} X^{(m)} \mid m, n \geq 0\}$	∞
\mathcal{U}_r	$\{Y^{(m_1)} \binom{H}{n} X^{(m_2)} \mid 0 \leq m_1, m_2, n \leq p^r - 1\}$	p^{3r}
\mathcal{U}_r^+	$\{X^{(m)} \mid 0 \leq m \leq p^r - 1\}$	p^r
\mathcal{U}_r^-	$\{Y^{(m)} \mid 0 \leq m \leq p^r - 1\}$	p^r
\mathcal{U}_r^0	$\{\binom{H}{n} \mid 0 \leq n \leq p^r - 1\}$	p^r
\mathcal{A}_r	$\{Y^{(m)} \binom{H}{n} X^{(m)} \mid 0 \leq m, n \leq p^r - 1\}$	p^{2r}

When performing calculations in $\mathcal{U}_{\mathbb{Z}}$ or \mathcal{U} , the following well-known formulas are often used.

Proposition 2.1. *Let $c \in \mathbb{Z}$ and $m, n \in \mathbb{Z}_{\geq 0}$. In $\mathcal{U}_{\mathbb{Z}}$, the following hold.*

$$\begin{aligned} X^{(m)}Y^{(n)} &= \sum_{i=0}^{\min(m,n)} Y^{(n-i)} \binom{H-m-n+2i}{i} X^{(m-i)}, \\ \binom{H+c}{m} X^{(n)} &= X^{(n)} \binom{H+c+2n}{m}, \\ \binom{H+c}{m} Y^{(n)} &= Y^{(n)} \binom{H+c-2n}{m}, \\ X^{(m)}X^{(n)} &= \binom{m+n}{n} X^{(m+n)}, \quad Y^{(m)}Y^{(n)} = \binom{m+n}{n} Y^{(m+n)}. \end{aligned}$$

In \mathcal{U} , the following formula, known as Lucas' theorem, also plays an important role.

Proposition 2.2. *Let $m, n \in \mathbb{Z}_{\geq 0}$. Let $m = \sum_{i \geq 0} m_i p^i$ and $n = \sum_{i \geq 0} n_i p^i$ be their p -adic expansions. Then we have*

$$\binom{m}{n} \equiv \prod_{i \geq 0} \binom{m_i}{n_i} \pmod{p}.$$

Let $\text{Fr} : \mathcal{U} \rightarrow \mathcal{U}$ be a k -algebra endomorphism defined by

$$\begin{aligned} X^{(n)} &\mapsto \begin{cases} X^{(n/p)} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases}, \quad Y^{(n)} \mapsto \begin{cases} Y^{(n/p)} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases} \\ \left(\text{then } \binom{H}{n} \right) &\mapsto \begin{cases} \binom{H}{n/p} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases}. \end{aligned}$$

There is an k -linear map $\text{Fr}' : \mathcal{U} \rightarrow \mathcal{U}$ defined by

$$Y^{(m_1)} \binom{H}{n} X^{(m_2)} \mapsto Y^{(m_1 p)} \binom{H}{np} X^{(m_2 p)}.$$

Clearly we have $\text{Fr} \circ \text{Fr}' = \text{id}_{\mathcal{U}}$. Fr' is not an k -algebra homomorphism, but $\text{Fr}'|_{\mathcal{U}^+}$, $\text{Fr}'|_{\mathcal{U}^-}$, and $\text{Fr}'|_{\mathcal{U}^0}$ are (see [1, Proposition 1.1 and Corollaire 1.2]).

3 Primitive idempotents in \mathcal{U}_r^0

To construct the elements $B^{(\epsilon)}(\mathbf{a}, j)$ of \mathcal{U}_r that we are seeking, primitive idempotents in \mathcal{U}_r^0 are required. For $a \in \mathbb{Z}$, set

$$\mu_a^{(r)} = \binom{H-a-1}{p^r-1} \in \mathcal{U}_r^0.$$

If $r = 1$, set $\mu_a = \mu_a^{(1)}$.

The following facts are easy to check (for details, see [2, 4.7]).

Proposition 3.1. *For $a \in \mathbb{Z}$, the following hold.*

(i) $\binom{H}{n} \mu_a^{(r)} = \binom{a}{n} \mu_a^{(r)}$ for any $n \in \{0, 1, \dots, p^r - 1\}$.

(ii) For $b \in \mathbb{Z}$, we have

$$\mu_a^{(r)} = \mu_b^{(r)} \iff a \equiv b \pmod{p^r}.$$

(iii) The elements $\mu_b^{(r)}$ with $b \in \{0, 1, \dots, p^r - 1\}$ are pairwise orthogonal primitive idempotents in \mathcal{U}_r^0 satisfying $\sum_{b=0}^{p^r-1} \mu_b^{(r)} = 1$.

4 The elements $B^{(\epsilon)}(a, j)$ in \mathcal{U}_1

Here, following Seligman [3], we construct the elements $B^{(\epsilon)}(a, j)$ in \mathcal{U}_1 . These are the specializations at $r = 1$ of the elements $B^{(\epsilon)}(\mathbf{a}, j)$ in \mathcal{U}_r constructed in the next section.

Suppose for a moment that p is odd. Set $\mathcal{S} = \{0, 1, \dots, (p-1)/2\} (\subset \mathbb{Z})$ and let $\overline{\mathcal{S}}$ be the image of \mathcal{S} under the natural map $\mathbb{Z} \rightarrow \mathbb{F}_p$. For $\epsilon \in \mathbb{F}_2 = \{0, 1\}$ and $j \in \mathcal{S}$, we define polynomials $\psi_j^{(\epsilon)}(x) \in \mathbb{F}_p[x]$ as

$$\psi_0^{(0)}(x) = \psi_0^{(1)}(x) = \prod_{i \in \overline{\mathcal{S}} \setminus \{0\}} (x - i^2)^2,$$

$$\psi_s^{(0)}(x) = 2x(x + s^2) \prod_{i \in \overline{\mathcal{S}} \setminus \{0, s\}} (x - i^2)^2 \quad (s \in \mathcal{S} \setminus \{0\}),$$

$$\psi_s^{(1)}(x) = x(x - s^2) \prod_{i \in \overline{\mathcal{S}} \setminus \{0, s\}} (x - i^2)^2 \quad (s \in \mathcal{S} \setminus \{0\}).$$

Set $\mathcal{P}_{\mathbb{Z}} = \mathbb{Z} \times \mathcal{S}$ and

$$B^{(\epsilon)}(a, j) = \psi_j^{(\epsilon)} \left(\mu_a Y X + \left(\frac{a+1}{2} \right)^2 \right) \cdot \mu_a \in \mathcal{A}_1$$

for $\varepsilon \in \mathbb{F}_2$ and $(a, j) \in \mathcal{P}_{\mathbb{Z}}$.

Suppose that $p = 2$. Then we consider the set

$$\mathcal{P}_{\mathbb{Z}} = \left\{ \left(2i, \frac{1}{2} \right), (1 + 2i, 0), (1 + 2i, 1) \mid i \in \mathbb{Z} \right\} \subset \mathbb{Z} \times \mathbb{Q}$$

and define $B^{(\varepsilon)}(a, j) \in \mathcal{A}_1$ as

$$B^{(0)}\left(2i, \frac{1}{2}\right) = \mu_0, \quad B^{(1)}\left(2i, \frac{1}{2}\right) = \mu_0 YX,$$

$$B^{(0)}(1 + 2i, 0) = B^{(1)}(1 + 2i, 0) = \mu_1 YX,$$

$$B^{(0)}(1 + 2i, 1) = B^{(1)}(1 + 2i, 1) = \mu_1 YX + \mu_1$$

for any $i \in \mathbb{Z}$.

Let p be an arbitrary prime number again. For $\varepsilon \in \mathbb{F}_2$ and $(a_1, j_1), (a_2, j_2) \in \mathcal{P}_{\mathbb{Z}}$, we have

$$B^{(\varepsilon)}(a_1, j_1) = B^{(\varepsilon)}(a_2, j_2) \iff a_1 \equiv a_2 \pmod{p} \text{ and } j_1 = j_2.$$

Set $\mathcal{P} = \{(a, j) \in \mathcal{P}_{\mathbb{Z}} \mid 0 \leq a \leq p - 1\}$. So we have

$$\mathcal{P} = \begin{cases} \{0, 1, \dots, p - 1\} \times \mathcal{S} & \text{if } p \neq 2, \\ \{(0, 1/2), (1, 0), (1, 1)\} & \text{if } p = 2 \end{cases}.$$

The following proposition is a result by Seligman and served as a motivation for our present study.

Proposition 4.1 ([3, Theorem 1]). *If $p \neq 2$, the elements $B^{(0)}(a, j)$ with $(a, j) \in \mathcal{P}$ are pairwise orthogonal primitive idempotents in \mathcal{U}_1 satisfying $\sum_{(a, j) \in \mathcal{P}} B^{(0)}(a, j) = 1$.*

5 The elements $B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$ in \mathcal{U}_r

In this section, we finally construct the elements $B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$ of \mathcal{U}_r that we are seeking. However, some further preparation is necessary before doing so.

For an integer $n \in \mathbb{Z}$, we denote by $n \bmod p$ a unique integer \hat{n} with $\hat{n} \equiv n \pmod{p}$ and $0 \leq \hat{n} \leq p - 1$. We classify pairs $(a, j) \in \mathcal{P}_{\mathbb{Z}}$ under the following four conditions:

- (A) \hat{a} is even and $(p - \hat{a} + 1)/2 \leq j \leq (p - 1)/2$,
- (B) \hat{a} is even and $0 \leq j \leq (p - \hat{a} - 1)/2$,
- (C) \hat{a} is odd and $0 \leq j \leq (\hat{a} - 1)/2$,
- (D) \hat{a} is odd and $(\hat{a} + 1)/2 \leq j \leq (p - 1)/2$,

where $\hat{a} = a \bmod p$.

Definition 5.1. Let $\varepsilon \in \mathbb{F}_2$ and $(a, j) \in \mathcal{P}_{\mathbb{Z}}$, and set $\widehat{a} = a \bmod p$. Then define nonnegative integers $n^{(\varepsilon)}(a, j)$ and $\widetilde{n}^{(\varepsilon)}(a, j)$ every condition of (a, j) from (A) to (D) as follows:

(a, j)	$n^{(0)}(a, j)$	$n^{(1)}(a, j)$	$\widetilde{n}^{(0)}(a, j)$	$\widetilde{n}^{(1)}(a, j)$
(A)	$\frac{p - \widehat{a} - 1}{2} + j$	$\frac{3p - \widehat{a} - 1}{2} - j$	$\frac{-p + \widehat{a} - 1}{2} + j$	$\frac{p + \widehat{a} - 1}{2} - j$
(B)	$\frac{p - \widehat{a} - 1}{2} - j$	$\frac{p - \widehat{a} - 1}{2} + j$	$\frac{p + \widehat{a} - 1}{2} - j$	$\frac{p + \widehat{a} - 1}{2} + j$
(C)	$\frac{2p - \widehat{a} - 1}{2} - j$	$\frac{2p - \widehat{a} - 1}{2} + j$	$\frac{\widehat{a} - 1}{2} - j$	$\frac{\widehat{a} - 1}{2} + j$
(D)	$j - \frac{\widehat{a} + 1}{2}$	$\frac{2p - \widehat{a} - 1}{2} - j$	$\frac{\widehat{a} - 1}{2} + j$	$\frac{2p + \widehat{a} - 1}{2} - j$

Apart from (A)-(D), we also consider the following condition for $(a, j) \in \mathcal{P}_{\mathbb{Z}}$:

(E) $j = 0$ if $p \neq 2$ or $a \equiv 1 \pmod{2}$ if $p = 2$.

Remark. For $(a, j) \in \mathcal{P}_{\mathbb{Z}}$ and $\varepsilon \in \mathbb{F}_2$, we easily see the following.

(a) $\widetilde{n}^{(\varepsilon)}(a, j) = n^{(\varepsilon)}(-a, j)$.

(b) $0 \leq n^{(0)}(a, j) \leq n^{(1)}(a, j) \leq p - 1$ and

$$n^{(0)}(a, j) = n^{(1)}(a, j) \iff (a, j) \text{ satisfies (E).}$$

(c) $n^{(0)}(a, j) + \widetilde{n}^{(1)}(a, j) = n^{(1)}(a, j) + \widetilde{n}^{(0)}(a, j) = p - 1$.

Lemma 5.2. Let $(a, j) \in \mathcal{P}_{\mathbb{Z}}$ and $\varepsilon \in \mathbb{F}_2$. Then the element $B^{(\varepsilon)}(a, j) \in \mathcal{U}_1$ can be written as

$$\begin{aligned} B^{(\varepsilon)}(a, j) &= \mu_a \sum_{m=n^{(\varepsilon)}(a, j)}^{p-1} c_m^{(\varepsilon)}(a, j) Y^m X^m \\ &= \mu_a \sum_{m=\widetilde{n}^{(\varepsilon)}(a, j)}^{p-1} \widetilde{c}_m^{(\varepsilon)}(a, j) X^m Y^m \end{aligned}$$

for some $c_m^{(\varepsilon)}(a, j), \widetilde{c}_m^{(\varepsilon)}(a, j) \in \mathbb{F}_p$ with $c_{n^{(\varepsilon)}(a, j)}^{(\varepsilon)}(a, j) \neq 0$ and $\widetilde{c}_{\widetilde{n}^{(\varepsilon)}(a, j)}^{(\varepsilon)}(a, j) \neq 0$.

Set $\widehat{a} = a \bmod p$. If $(a, j) \in \mathcal{P}_{\mathbb{Z}}$ satisfies (A) or (C), then define an integer $s(a, j)$ as

$$s(a, j) = \begin{cases} \frac{p-\widehat{a}+1}{2} & \text{if } p \neq 2 \text{ and } \widehat{a} \text{ is even,} \\ \frac{p-\widehat{a}}{2} & \text{if } p \neq 2 \text{ and } \widehat{a} \text{ is odd,} \\ 1 & \text{if } p = 2 \end{cases}.$$

For $\varepsilon \in \mathbb{F}_2$ and $(a, j) \in \mathcal{P}_{\mathbb{Z}}$, we write

$$B^{(\varepsilon)}(a, j) = \mu_a \sum_{m=n^{(\varepsilon)}(a, j)}^{p-1} c_m^{(\varepsilon)}(a, j) Y^m X^m$$

following the previous lemma.

Then we define $Z^{(\varepsilon)}(z; (a, j))$ for $z \in \mathcal{U}$ as

$$Z^{(\varepsilon)}(z; (a, j)) = \mu_a \sum_{m=n^{(\varepsilon)}(a, j)}^{p-1} c_m^{(\varepsilon)}(a, j) Y^m X^{m-s(a, j)} \text{Fr}'(z) X^{s(a, j)}$$

if (a, j) satisfies (A) or (C), and

$$Z^{(\varepsilon)}(z; (a, j)) = \text{Fr}'(z) B^{(\varepsilon)}(a, j) \quad (= B^{(\varepsilon)}(a, j) \text{Fr}'(z))$$

if (a, j) satisfies (B) or (D).

Consider $((a_i, j_i))_{i=0}^{r-1} = ((a_0, j_0), \dots, (a_{r-1}, j_{r-1})) \in \mathcal{P}_{\mathbb{Z}}^r$. For convenience we shall write it as

$$((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$$

or (\mathbf{a}, \mathbf{j}) with $\mathbf{a} = (a_0, \dots, a_{r-1})$ and $\mathbf{j} = (j_0, \dots, j_{r-1})$.

We are now finally ready to define the elements $B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$. For $\varepsilon = (\varepsilon_0, \dots, \varepsilon_{r-1}) \in \mathbb{F}_2^r$, $(\mathbf{a}, \mathbf{j}) = ((a_i, j_i))_{i=0}^{r-1} \in \mathcal{P}_{\mathbb{Z}}^r$ and $z \in \mathcal{U}$, we define an element $Z^{(\varepsilon)}(z; (\mathbf{a}, \mathbf{j})) \in \mathcal{U}$ inductively as

$$Z^{(\varepsilon)}(z; (\mathbf{a}, \mathbf{j})) = \begin{cases} Z^{(\varepsilon_0)}(z; (a_0, j_0)) & \text{if } r = 1, \\ Z^{(\varepsilon_0)}(Z^{(\varepsilon')} (z; (\mathbf{a}', \mathbf{j}')) ; (a_0, j_0)) & \text{if } r \geq 2 \end{cases},$$

where $\varepsilon' = (\varepsilon_1, \dots, \varepsilon_{r-1})$ and $(\mathbf{a}', \mathbf{j}') = ((a_i, j_i))_{i=1}^{r-1}$. Then set $B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = Z^{(\varepsilon)}(1; (\mathbf{a}, \mathbf{j})) \in \mathcal{A}_r$.

Set $\mathbf{0} = (0, \dots, 0)$, $\mathbf{1} = (1, \dots, 1) \in \mathbb{F}_2^r$. The following theorem is a generalization of Proposition 4.1.

Theorem 5.3 ([5, Proposition 5.5 (iii)]). *The elements $B^{(\mathbf{0})}(\mathbf{a}, \mathbf{j})$ with $(\mathbf{a}, \mathbf{j}) \in \mathcal{P}^r$ are pairwise orthogonal primitive idempotents in \mathcal{U}_r and \mathcal{A}_r satisfying $\sum_{(\mathbf{a}, \mathbf{j}) \in \mathcal{P}^r} B^{(\mathbf{0})}(\mathbf{a}, \mathbf{j}) = 1$. In particular, $\mathcal{U}_r B^{(\mathbf{0})}(\mathbf{a}, \mathbf{j})$ and $\mathcal{A}_r B^{(\mathbf{0})}(\mathbf{a}, \mathbf{j})$ are projective indecomposable modules for \mathcal{U}_r and \mathcal{A}_r respectively.*

For $(a, j) \in \mathcal{P}_{\mathbb{Z}}$, $i \in \mathbb{Z}$, and $n \in \{0, 1, \dots, p-1\}$, define $\gamma_i(a, j)$, $\tilde{\gamma}_i(a, j)$, $\beta_n(a, j)$, and $\tilde{\beta}_n(a, j)$ in \mathbb{F}_p as follows:

$$\gamma_i(a, j) = j^2 - \left(\frac{a+1}{2}\right)^2 - i(i+a+1) \left(= j^2 - \left(\frac{a+1}{2} + i\right)^2\right),$$

$$\tilde{\gamma}_i(a, j) = \gamma_i(-a, j),$$

$$\beta_n(a, j) = \prod_{i=0}^{n-1} \gamma_i(a, j),$$

$$\tilde{\beta}_n(a, j) = \beta_n(-a, j) \left(= \prod_{i=0}^{n-1} \tilde{\gamma}_i(a, j)\right).$$

Here if $p = 2$, $\gamma_i(a, j)$ is defined by regarding the right-hand side (which is an integer in this situation) as the image under the natural map $\mathbb{Z} \rightarrow \mathbb{F}_2$. Clearly we have $\beta_0(a, j) = \tilde{\beta}_0(a, j) = 1$ by definition. For $i \in \mathbb{Z}$ and $s \in \mathbb{Z}_{\geq 0}$, we have

$$\gamma_{i+s}(a, j) = \gamma_i(a + 2s, j),$$

$$\tilde{\gamma}_{i+s}(a, j) = \tilde{\gamma}_i(a - 2s, j)$$

by definition. Moreover, if $0 \leq i \leq p-1$, we have

$$\gamma_i(a, j) = 0 \iff i \in \{n^{(0)}(a, j), n^{(1)}(a, j)\},$$

$$\tilde{\gamma}_i(a, j) = 0 \iff i \in \{\tilde{n}^{(0)}(a, j), \tilde{n}^{(1)}(a, j)\}.$$

Let us state some properties of the elements $B^{(\epsilon)}(\mathbf{a}, \mathbf{j})$.

Proposition 5.4. *Let $(\mathbf{a}, \mathbf{j}) = ((a_i, j_i))_{i=0}^{r-1} \in \mathcal{P}_{\mathbb{Z}}^r$ and $\epsilon = (\epsilon_0, \dots, \epsilon_{r-1}) \in \mathbb{F}_2^r$. The following hold.*

(i) $\binom{H}{n} B^{(\epsilon)}(\mathbf{a}, \mathbf{j}) = \left(\sum_{i=0}^{r-1} p^{i b_i}\right) B^{(\epsilon)}(\mathbf{a}, \mathbf{j})$ for $0 \leq n \leq p^r - 1$, where

$$b_i = \begin{cases} a_i \bmod p - p & \text{if } (a_i, j_i) \text{ satisfies (A) or (C)} \\ a_i \bmod p & \text{if } (a_i, j_i) \text{ satisfies (B) or (D)} \end{cases}.$$

(ii) For $0 \leq i \leq r-1$, we have

$$Y^{(p^i)s} X^{(p^i)s} B^{(\epsilon)}(\mathbf{a}, \mathbf{j}) = \beta_s(a_i, j_i) B^{(\epsilon)}(\mathbf{a}, \mathbf{j}) + 4j_i^2 \sum_{l=0}^{s-1} \frac{\beta_l(a_i, j_i)}{\gamma_l(a_i, j_i)} B^{(\epsilon + \mathbf{e}_{i+1})}(\mathbf{a}, \mathbf{j}),$$

$$X^{(p^i)t} Y^{(p^i)t} B^{(\epsilon)}(\mathbf{a}, \mathbf{j}) = \tilde{\beta}_t(a_i, j_i) B^{(\epsilon)}(\mathbf{a}, \mathbf{j}) + 4j_i^2 \sum_{l=0}^{t-1} \frac{\tilde{\beta}_l(a_i, j_i)}{\tilde{\gamma}_l(a_i, j_i)} B^{(\epsilon + \mathbf{e}_{i+1})}(\mathbf{a}, \mathbf{j})$$

if $\varepsilon_i = 0$, $0 \leq s \leq n^{(0)}(a_i, j_i)$, and $0 \leq t \leq \tilde{n}^{(0)}(a_i, j_i)$,

$$Y^{(p^i)s} X^{(p^i)s} B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = 4j_i^2 \left(\prod_{l=0, l \neq n^{(0)}(a_i, j_i)}^{s-1} \gamma_l(a_i, j_i) \right) B^{(\varepsilon + \mathbf{e}_{i+1})}(\mathbf{a}, \mathbf{j}),$$

$$X^{(p^i)t} Y^{(p^i)t} B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = 4j_i^2 \left(\prod_{l=0, l \neq \tilde{n}^{(0)}(a_i, j_i)}^{t-1} \tilde{\gamma}_l(a_i, j_i) \right) B^{(\varepsilon + \mathbf{e}_{i+1})}(\mathbf{a}, \mathbf{j})$$

if $\varepsilon_i = 0$, $n^{(0)}(a_i, j_i) < s \leq p-1$, and $\tilde{n}^{(0)}(a_i, j_i) < t \leq p-1$, and

$$Y^{(p^i)s} X^{(p^i)s} B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = \beta_s(a_i, j_i) B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}),$$

$$X^{(p^i)t} Y^{(p^i)t} B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = \tilde{\beta}_t(a_i, j_i) B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$$

if $\varepsilon_i = 1$ and $0 \leq s, t \leq p-1$.

(iii) We have

$$B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) B^{(0)}(\mathbf{a}, \mathbf{j}) = B^{(0)}(\mathbf{a}, \mathbf{j}) B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}).$$

(iv) For $\tilde{\varepsilon} = (\tilde{\varepsilon}_0, \dots, \tilde{\varepsilon}_{r-1}) \in \mathbb{F}_2^r$, we have

$$B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = B^{(\tilde{\varepsilon})}(\mathbf{a}, \mathbf{j}) \iff \varepsilon_i = \tilde{\varepsilon}_i \text{ whenever } (a_i, j_i) \text{ does not satisfy (E).}$$

(v) For $(\tilde{\mathbf{a}}, \tilde{\mathbf{j}}) = \left((\tilde{a}_i, \tilde{j}_i) \right)_{i=0}^{r-1} \in \mathcal{P}_{\mathbb{Z}}^r$, we have

$$B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = B^{(\varepsilon)}(\tilde{\mathbf{a}}, \tilde{\mathbf{j}}) \iff a_i \equiv \tilde{a}_i \pmod{p} \text{ and } j_i = \tilde{j}_i \text{ for each } i.$$

6 Some applications

In this section, we give some results obtained through the study of the elements $B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$. To begin with, as a preparation, we introduce some notation.

Definition 6.1. Let $(\mathbf{a}, \mathbf{j}) = ((a_i, j_i))_{i=0}^{r-1} \in \mathcal{P}_{\mathbb{Z}}^r$.

(1) For $\varepsilon = (\varepsilon_0, \dots, \varepsilon_{r-1})$, $\tilde{\varepsilon} = (\tilde{\varepsilon}_0, \dots, \tilde{\varepsilon}_{r-1}) \in \mathbb{F}_2^r$, define $\varepsilon \leq \tilde{\varepsilon}$ if $\varepsilon_i \leq \tilde{\varepsilon}_i$ for each i , regarding ε_i and $\tilde{\varepsilon}_i$ as the corresponding integers (i.e. 0 or 1 in \mathbb{Z}). This gives a partial order in \mathbb{F}_2^r .

(2) Two subsets $\mathcal{X}_r(\mathbf{a}, \mathbf{j})$ and $\mathcal{Y}_r(\mathbf{a}, \mathbf{j})$ of \mathbb{F}_2^r are defined as

$$\mathcal{X}_r(\mathbf{a}, \mathbf{j}) = \{(\varepsilon_0, \dots, \varepsilon_{r-1}) \in \mathbb{F}_2^r \mid \varepsilon_i = 0 \text{ whenever } (a_i, j_i) \text{ satisfies (E)}\},$$

$$\mathcal{Y}_r(\mathbf{a}, \mathbf{j}) = \{(\varepsilon_0, \dots, \varepsilon_{r-1}) \in \mathbb{F}_2^r \mid \varepsilon_i = 1 \text{ whenever } (a_i, j_i) \text{ satisfies (E)}\}.$$

(Each of $\mathcal{X}_r(\mathbf{a}, \mathbf{j})$ and $\mathcal{Y}_r(\mathbf{a}, \mathbf{j})$ is used to remove duplicates from the elements $B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$ with $\varepsilon \in \mathbb{F}_2^r$.)

(3) For $\varepsilon \in \mathcal{Y}_r(\mathbf{a}, \mathbf{j})$, define a subset $\widehat{\Theta}_r((\mathbf{a}, \mathbf{j}), \varepsilon)$ of $\mathbb{F}_2^r \times \mathbb{Z}^r$ as

$$\widehat{\Theta}_r((\mathbf{a}, \mathbf{j}), \varepsilon) = \left\{ (\boldsymbol{\theta}, \mathbf{t}(\boldsymbol{\theta})) \mid \begin{array}{l} \varepsilon \leq \boldsymbol{\theta} \in \mathcal{Y}_r(\mathbf{a}, \mathbf{j}) \text{ and} \\ -\widetilde{n}^{(\theta_i+1)}(a_i, j_i) \leq t_i(\theta_i) \leq n^{(\theta_i+1)}(a_i, j_i) \text{ for each } i \end{array} \right\},$$

where $\boldsymbol{\theta} = (\theta_0, \dots, \theta_{r-1}) \in \mathbb{F}_2^r$, $\mathbf{t}(\boldsymbol{\theta}) = (t_0(\theta_0), \dots, t_{r-1}(\theta_{r-1})) \in \mathbb{Z}^r$.

(4) For $i \in \mathbb{Z}_{\geq 0}$ and $t \in \mathbb{Z}$, define an element $u^{(i,t)}$ in \mathcal{U} as

$$u^{(i,t)} = \begin{cases} X^{(p^i)t} & \text{if } t \geq 0, \\ \left(Y^{(p^i)}\right)^{-t} & \text{if } t < 0 \end{cases}.$$

Moreover, for $\varepsilon = (\varepsilon_0, \dots, \varepsilon_{r-1}) \in \mathbb{F}_2^r$ and $\mathbf{t} = (t_0, \dots, t_{r-1}) \in \mathbb{Z}^r$, define an element $B^{(\varepsilon)}((\mathbf{a}, \mathbf{j}); \mathbf{t})$ in \mathcal{U}_r as

$$B^{(\varepsilon)}((\mathbf{a}, \mathbf{j}); \mathbf{t}) = u^{(0,t_0)} u^{(1,t_1)} \dots u^{(r-1,t_{r-1})} B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}).$$

(5) For $\varepsilon \in \mathcal{Y}_r(\mathbf{a}, \mathbf{j})$, define a subset $\widehat{\mathcal{B}}_r((\mathbf{a}, \mathbf{j}), \varepsilon)$ of \mathcal{U}_r as

$$\widehat{\mathcal{B}}_r((\mathbf{a}, \mathbf{j}), \varepsilon) = \left\{ B^{(\boldsymbol{\theta})}((\mathbf{a}, \mathbf{j}); \mathbf{t}(\boldsymbol{\theta})) \mid (\boldsymbol{\theta}, \mathbf{t}(\boldsymbol{\theta})) \in \widehat{\Theta}_r((\mathbf{a}, \mathbf{j}), \varepsilon) \right\}.$$

The following proposition says that the order of the elements ε in each of $\mathcal{X}_r(\mathbf{a}, \mathbf{j})$ and $\mathcal{Y}_r(\mathbf{a}, \mathbf{j})$ defined in Definition 6.1 (1) corresponds to the inclusion relation among the \mathcal{U}_r -modules $\mathcal{U}_r B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$.

Proposition 6.2 ([7, Remark (g) of Definition 4.1]). *For $\varepsilon, \rho \in \mathcal{Y}_r(\mathbf{a}, \mathbf{j})$, we have*

$$\mathcal{U}_r B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) \subseteq \mathcal{U}_r B^{(\rho)}(\mathbf{a}, \mathbf{j}) \iff \varepsilon \geq \rho,$$

$$\mathcal{U}_r B^{(\varepsilon)}(\mathbf{a}, \mathbf{j}) = \mathcal{U}_r B^{(\rho)}(\mathbf{a}, \mathbf{j}) \iff \varepsilon = \rho.$$

Moreover, these equivalences also hold for $\varepsilon, \rho \in \mathcal{X}_r(\mathbf{a}, \mathbf{j})$.

Let $\{L(\lambda) \mid \lambda \in \mathbb{Z}_{\geq 0}\}$ be the set of isomorphism classes of simple \mathcal{U} -modules. Then $\{L(\lambda) \mid 0 \leq \lambda \leq p^r - 1\}$ is the set of isomorphism classes of simple \mathcal{U}_r -modules.

The following theorem is about the structure of the \mathcal{U}_r -module $\mathcal{U}_r B^{(\varepsilon)}(\mathbf{a}, \mathbf{j})$.

Theorem 6.3 ([7, Theorems 5.1 and 5.3 and Corollary 5.6]). Let $(\mathbf{a}, \mathbf{j}) = ((a_i, j_i))_{i=0}^{r-1} \in \mathcal{P}_{\mathbb{Z}}^r$.

- (i) For $\boldsymbol{\varepsilon} \in \mathcal{Y}_r(\mathbf{a}, \mathbf{j})$, the set $\widehat{\mathcal{B}}_r((\mathbf{a}, \mathbf{j}), \boldsymbol{\varepsilon})$ forms a k -basis of the \mathcal{U}_r -module $\mathcal{U}_r B^{(\boldsymbol{\varepsilon})}(\mathbf{a}, \mathbf{j})$.
- (ii) $\mathcal{U}_r B^{(1)}(\mathbf{a}, \mathbf{j})$ is a simple \mathcal{U}_r -module which is isomorphic to $L(\sum_{i=0}^{r-1} p^i \kappa_i)$, where

$$\kappa_i = \begin{cases} 2j_i - 1 & \text{if } (a_i, j_i) \text{ satisfies (A) or (D),} \\ p - 2j_i - 1 & \text{if } (a_i, j_i) \text{ satisfies (B) or (C)} \end{cases}.$$

- (iii) For $\boldsymbol{\varepsilon} \in \mathbb{F}_2^r$, the \mathcal{U}_r -module $\mathcal{U}_r B^{(\boldsymbol{\varepsilon})}(\mathbf{a}, \mathbf{j})$ has head and socle isomorphic to the simple \mathcal{U}_r -module $\mathcal{U}_r B^{(1)}(\mathbf{a}, \mathbf{j})$.

If p is odd, set

$$h(\nu, i) = \binom{H + 2p^i \nu}{2p^i \nu} + \binom{H + 2p^i \nu - 1}{2p^i \nu} \in \mathcal{U}_{i+1}^0$$

for $\nu \in \{1, 2, \dots, (p-1)/2\}$ and $i \in \mathbb{Z}_{\geq 0}$.

The following theorem is a generalization of Wong [4, Main theorem].

Theorem 6.4 ([8, Theorem 4.1]). (i) Suppose that p is odd. Let ν_l be integers with $1 \leq \nu_l \leq (p-1)/2$ for $l \in \{0, \dots, r-1\}$. Then the set

$$\left\{ h(\nu_i, i) X^{(p^i)p-\nu_i}, Y^{(p^i)p-\nu_i} h(\nu_i, i) \mid 0 \leq i \leq r-1 \right\}$$

generates the Jacobson radical $\text{rad} \mathcal{U}_r$ as a two-sided ideal of \mathcal{U}_r .

- (ii) Suppose that $p = 2$. Then the set

$$\{\mu_m^{(i+1)} X^{(m)} X^{(2^i)}, Y^{(2^i)} Y^{(m)} \mu_m^{(i+1)} \mid 0 \leq i \leq r-1, 0 \leq m \leq 2^i - 1\}$$

generates the Jacobson radical $\text{rad} \mathcal{U}_r$ as a two-sided ideal of \mathcal{U}_r .

For $\boldsymbol{\varepsilon} = (\varepsilon_0, \dots, \varepsilon_{r-1}) \in \mathbb{F}_2^r$, set $\mathcal{W}(\boldsymbol{\varepsilon}) = \#\{i \mid \varepsilon_i = 1\}$. For $(\mathbf{a}, \mathbf{j}) = ((a_i, j_i))_{i=0}^{r-1} \in \mathcal{P}_{\mathbb{Z}}^r$, set $w = \#\{i \mid (a_i, j_i) \text{ does not satisfy (E)}\}$.

$\mathcal{A}_r \cdot B^{(0)}(\mathbf{a}, \mathbf{j})$ is a commutative k -algebra. Actually, the radical series of the algebra can be written in terms of the elements $B^{(\boldsymbol{\varepsilon})}(\mathbf{a}, \mathbf{j})$ with $\boldsymbol{\varepsilon} \in \mathcal{X}_r(\mathbf{a}, \mathbf{j})$.

Theorem 6.5 ([6, Proposition 3.10]). *For a positive integer i , we have*

$$\begin{aligned} (\text{rad}(\mathcal{A}_r \cdot B^{(0)}(\mathbf{a}, \mathbf{j})))^i &= \sum_{\theta \in \mathcal{X}_r(\mathbf{a}, \mathbf{j}), \mathcal{W}(\theta)=i} \mathcal{A}_r \cdot B^{(\theta)}(\mathbf{a}, \mathbf{j}) \\ &= \sum_{\theta \in \mathcal{X}_r(\mathbf{a}, \mathbf{j}), \mathcal{W}(\theta) \geq i} k \cdot B^{(\theta)}(\mathbf{a}, \mathbf{j}). \end{aligned}$$

In particular, $(\text{rad}(\mathcal{A}_r \cdot B^{(0)}(\mathbf{a}, \mathbf{j})))^i = 0$ if and only if $i > w$.

References

- [1] M. Gros and M. Kaneda, *Contraction par Frobenius de G -modules*, Ann. Inst. Fourier **61** (2011), 2507–2542.
- [2] M. Gros and M. Kaneda, *Un scindage du morphisme de Frobenius quantique*, Ark. Mat. **53** (2015), 271–301.
- [3] G. B. Seligman, *On idempotents in reduced enveloping algebras*, Trans. Amer. Math. Soc. **355** (2003), 3291–3300.
- [4] K. C. Wong, *The radical of the restricted universal enveloping algebra of A_1* , Rocky Mountain J. Math. **13** (1983), 215–221.
- [5] Y. Yoshii, *Primitive idempotents of the hyperalgebra for the r -th Frobenius kernel of $\text{SL}(2, k)$* , J. Lie Theory **27** (2017), 995–1026.
- [6] Y. Yoshii, *Projective modules for the subalgebra of degree 0 in a finite-dimensional hyperalgebra of type A_1* , Proc. Amer. Math. Soc. **146** (2018), 1977–1989.
- [7] Y. Yoshii, *A basis of a certain module for the hyperalgebra of $(\text{SL}_2)_r$ and some applications*, to appear in J. Algebra Appl. (2022) 2250184.
- [8] Y. Yoshii, *Generating sets of the Jacobson radical of the hyperalgebra of $(\text{SL}_2)_r$* , Journal of Computational Algebra **9** (2024), No. 100011.

College of Education, Ibaraki University
 2-1-1 Bunkyo, Mito, Ibaraki, 310-8512, Japan
 E-mail address: yutaka.yoshii.6174@vc.ibaraki.ac.jp