Journal of Lie Theory
Volume **27** (2017) 529–544

Cohomology of $\mathbb{N}$-Graded Lie Algebras of Maximal Class over $\mathbb{Z}_2$

Yuri Nikolayevsky* **and Ioannis Tsartsaflis**

Communicated by A. Fialowski

Abstract. We compute the cohomology with trivial coefficients of Lie algebras $\mathfrak{m}_0$ and $\mathfrak{m}_2$ of maximal class over the field $\mathbb{Z}_2$. In the infinite-dimensional case, we show that the cohomology rings $H^*(\mathfrak{m}_0)$ and $H^*(\mathfrak{m}_2)$ are isomorphic, in contrast with the case of the ground field of characteristic zero, and we obtain a complete description of them. In the finite-dimensional case, we find the first three Betti numbers of $\mathfrak{m}_0(n)$ and $\mathfrak{m}_2(n)$ over $\mathbb{Z}_2$.
Mathematics Subject Classification 2010: 17B56, 17B50, 17B70, 17B65, 17B30.
Key Words and Phrases: Lie algebra of maximal class, characteristic 2, cohomology, Betti number.

1. Introduction

A Lie algebra $\mathfrak{g}$ is said to be $\mathbb{N}$-*graded*, if it is the direct sum of subspaces $\mathfrak{g}_i$, $i \in \mathbb{N}$ (the *homogeneous components*), such that $[\mathfrak{g}_i, \mathfrak{g}_j] \subset \mathfrak{g}_{i+j}$. Obviously, finite-dimensional $\mathbb{N}$-graded Lie algebras are necessarily nilpotent. A great deal of attention in the literature has been focused on $\mathbb{N}$-graded Lie algebras for which the homogeneous components $\mathfrak{g}_i$ are "the smallest possible", that is, all of dimension one or, in the finite-dimensional case, $\dim \mathfrak{g}_i = 1$, for $i \le n := \dim \mathfrak{g}$, and $\mathfrak{g}_i = 0$, for $i > n$. With the additional condition that $\mathfrak{g}$ is generated as an algebra by elements e_1 and e_2, spanning $\mathfrak{g}_1$ and $\mathfrak{g}_2$ respectively, one obtains that the subspaces $C_0 = \mathfrak{g}$, $C_k = \oplus_{i=k+2}^{\infty} \mathfrak{g}_i$, $k > 0$, are the terms of the central descending series. This defines the $\mathbb{N}$-graded filiform Lie algebras in the finite-dimensional case [15] and the $\mathbb{N}$-graded Lie algebras of maximal class [12] (also called *narrow* algebras). In characteristic zero, these algebras have been completely classified. In the infinite-dimensional case, one gets just three algebras [6]. We list them here with their presentations:

$$\mathfrak{m}_0 = \mathrm{Span}(e_1, e_2, \dots), \qquad [e_1, e_i] = e_{i+1},\ i > 1, \tag{1}$$
$$\mathfrak{m}_2 = \mathrm{Span}(e_1, e_2, \dots), \qquad [e_1, e_i] = e_{i+1},\ i > 1, \quad [e_2, e_j] = e_{j+2},\ j > 2, \tag{2}$$
$$\mathcal{V} = \mathrm{Span}(e_1, e_2, \dots), \qquad [e_i, e_j] = (j - i)e_{i+j},\ i, j \ge 1. \tag{3}$$

* Partially supported by ARC Discovery grant DP130103485.

ISSN 0949–5932 / \$2.50

In the finite-dimensional case in characteristic zero, the classification of finite-dimensional $\mathbb{N}$-graded filiform Lie algebras was established in [10]: one obtains the "truncations" of the above three algebras, in particular,

$$\mathfrak{m}_0(n) = \mathrm{Span}(e_1, \dots, e_n),\ [e_1, e_i] = e_{i+1},\ 1 < i < n, \tag{4}$$

$$\mathfrak{m}_2(n) = \mathrm{Span}(e_1, \dots, e_n),\ [e_1, e_i] = e_{i+1},\ 1 < i < n, \quad [e_2, e_j] = e_{j+2},\ 2 < j < n-1, \tag{5}$$

and $\mathcal{V}(n)$, plus another three infinite series, and five one-parameter families of low-dimensional algebras. The picture is more complicated in positive characteristic: by [4], there are uncountably many isomorphism classes of Lie algebras of maximal class; the construction of all such algebras in odd characteristic is given in [5], and in characteristic two, in [9], with $\mathfrak{m}_0$ and $\mathfrak{m}_2$ being the simplest possible cases.

The cohomology of $\mathbb{N}$-graded Lie algebras of maximal class has been studied extensively over a field of characteristic zero [6, 7, 15], and at present is well-understood. In [7], Fialowski and Millionschikov gave a full description of the cohomology with trivial coefficients of the algebras $\mathfrak{m}_0$ and $\mathfrak{m}_2$; the Betti numbers of $\mathcal{V}$ are found in [8]. In the finite-dimensional case, the cohomology of $\mathfrak{m}_0(n)$ were found in [2] (see also [1] and [7]). However, already for $\mathfrak{m}_2(n)$ over a field of characteristic zero, our present knowledge is limited to the first two Betti numbers [10, 15].

The study of the cohomology of Lie algebras of maximal class over fields of positive characteristic is much less developed. The cohomology of the Heisenberg algebra is found in [3, 13]. A recent result by Tsartsarflis [14] states that over a field of characteristic two, the algebras $\mathfrak{m}_0(n)$ and $\mathfrak{m}_2(n)$ have the same Betti numbers (in contrast with the case of characteristic zero), and furthermore, every algebra of the so called *Vergne class* admits a dual, non-isomorphic algebra, with the same Betti numbers.

In this paper we study the cohomology with trivial coefficients of the Lie algebras $\mathfrak{m}_0$ and $\mathfrak{m}_2$, and their finite dimensional truncations, $\mathfrak{m}_0(n)$ and $\mathfrak{m}_2(n)$, over the field $\mathbb{Z}_2$. Let $V = \mathrm{Span}(e_1, e_2, \dots)$ and let $\{e^i\}$ be the dual basis for V^*. Define the operator D_1 on V^* by $D_1 e^1 = D_1 e^2 = 0$, $D_1 e^i = e^{i-1}$, for $i > 2$, and extend it to $\Lambda(V)$ as a derivation. For $\omega \in \Lambda(V)$ and $e^i \in V^*$, define $F(\omega, e^i) = \sum_{l=0}^{\infty} (D_1^l \omega) \wedge e^{i+l+1}$ (note that the sum on the right-hand side is finite).

Our main result in the infinite-dimensional case is as follows.

Theorem 1.1. *The cohomology rings $H^*(\mathfrak{m}_0)$ and $H^*(\mathfrak{m}_2)$ over the field $\mathbb{Z}_2$ are isomorphic. The respective cohomology classes of the cocycles*

$$e^1,\ e^2,\ F(e^{i_1} \wedge e^{i_2} \wedge \dots \wedge e^{i_q}, e^{i_q}), \tag{6}$$

where $q \geq 1$, $2 \leq i_1 < i_2 < \ldots < i_q$, form a basis for $H^*(\mathfrak{m}_0)$ and for $H^*(\mathfrak{m}_2)$, respectively.

Note that $H^*(\mathfrak{m}_0)$ over $\mathbb{Z}_2$ is "the same" as over a field of characteristic zero (compare with [7, Theorem 3.4]). In contrast, the fact that $H^*(\mathfrak{m}_0)$ and $H^*(\mathfrak{m}_2)$ over $\mathbb{Z}_2$ are isomorphic (note that $\mathfrak{m}_0$ and $\mathfrak{m}_2$ are not isomorphic over any ground field) is specific to the $\mathbb{Z}_2$ case: over a field of characteristic zero, $H^*(\mathfrak{m}_2)$ is very different [7, Theorem 5.5].

In the finite-dimensional case, which appears to be substantially harder that the infinite-dimensional one, we compute the first three Betti numbers of $\mathfrak{m}_0(n)$ and the corresponding bases for $H^i(\mathfrak{m}_0(n))$, $i = 1, 2, 3$.

Theorem 1.2. *The first three Betti numbers of the Lie algebra* $\mathfrak{m}_0(n)$ *over* $\mathbb{Z}_2$ *are given by*

(a) $b_1(\mathfrak{m}_0(n)) = 2$,

(b) $b_2(\mathfrak{m}_0(n)) = \lfloor \frac{1}{2}(n+1) \rfloor$, *where* $\lfloor . \rfloor$ *denotes the integer part,*

(c) $b_3(\mathfrak{m}_0(n)) = \frac{1}{3}(2^p - 1)(2^{p-1} - 1) + \frac{1}{2}m(m-1) + \lfloor \frac{1}{2}(n-1) \rfloor$, *where* $n = 2^p + m$ *and* $0 < m \leq 2^p$.

An explicit form of the basis for $H^3(\mathfrak{m}_0(n))$ is given in Theorem 3.8 of Section 3. Theorem 1.2 also gives us the first three Betti numbers of $\mathfrak{m}_2(n)$ (Corollary 4.1 of Section 4), which in characteristic two are simply the same as those for $\mathfrak{m}_0(n)$, by [14, Theorem 1].

The paper is organised as follows. We begin with some short preliminaries in Section 2. We treat the algebras $\mathfrak{m}_0$ and $\mathfrak{m}_0(n)$ in Section 3. Parts (a) and (b) of Theorem 1.2 follow from Proposition 3.3. After some technical preparation similar to the arguments of [7], we prove Theorem 3.2, which is "the $\mathfrak{m}_0$-part" of Theorem 1.1. We then proceed to the proof of Theorem 1.2(c). This is the longest and most technically involved part of the paper. Finally, in Section 4 we use a construction similar to [14] to establish the isomorphism between $H^*(\mathfrak{m}_0)$ and $H^*(\mathfrak{m}_2)$, hence completing the proof of Theorem 1.1.

2. Preliminaries

Given a Lie algebra $\mathfrak{g}$ over $\mathbb{Z}_2$ with a basis elements e_i, we denote the dual basis elements e^i. For convenience, we set $e^0 = 0$. For simplicity we write a monomial q-form $e^{i_1} \wedge e^{i_2} \wedge \cdots \wedge e^{i_q} \in \Lambda^q(\mathfrak{g})$ as $e^{i_1 i_2 \dots i_q}$. For a monomial $e^{i_1 i_2 \dots i_q}$, its *degree* is defined to be $\sum_{j=1}^q i_j$. The *homogeneous component* $\Lambda^q_k(\mathfrak{g})$ of degree k and of rank q is the span of all the monomials of degree k and of rank q. We set $\Lambda_k(\mathfrak{g}) := \oplus_q \Lambda^q_k(\mathfrak{g})$.

As usual, the *differential* d is defined by $d\xi(X, Y) = \xi[X, Y]$ for one-forms ξ, where $X, Y \in \mathfrak{g}$, and then is extended to the exterior algebra $\Lambda(\mathfrak{g})$ as a derivation (so that $d(\omega_1 \wedge \omega_2) = d(\omega_1) \wedge \omega_2 + \omega_1 \wedge d(\omega_2)$). Then $d^2 = 0$ and one define the *q-th cohomology group* $H^q(\mathfrak{g})$ (with trivial coefficients) by $H^q(\mathfrak{g}) = \ker(d : \Lambda^q \to \Lambda^{q+1})/\mathrm{Im}\,(d : \Lambda^{q-1} \to \Lambda^q)$. Then $H^q(\mathfrak{g})$ is a linear space over $\mathbb{Z}_2$; if its dimension is finite, it is called the *q-th Betti number* $b_q(\mathfrak{g})$. It is immediate from the definition that if $\dim \mathfrak{g} = n$, then

$$b_q(\mathfrak{g}) = \dim \ker(d : \Lambda^q \to \Lambda^{q+1}) + \dim \ker(d : \Lambda^{q-1} \to \Lambda^q) - \binom{n}{q-1}, \qquad (7)$$

so to compute the Betti numbers it suffices to know the dimensions of the kernels of d on the Λ^q's. Also note that in the graded case (in particular, for the bases $\{e_i\}$ from (1 – 5)), the operator d maps $\Lambda^q_k(\mathfrak{g})$ to $\Lambda^{q+1}_k(\mathfrak{g})$, and so $H^q(\mathfrak{g})$ is spanned by the classes of homogeneous elements; we get a decomposition (a bi-gradation) $H^q(\mathfrak{g}) = \oplus_k H^q_k(\mathfrak{g})$. The multiplicative structure in $H(\mathfrak{g}) := \oplus_q H^q(\mathfrak{g})$ is inherited from the wedge product.

3. Cohomology of $\mathfrak{m}_0$

In this section, we compute the cohomology of the infinite-dimensional Lie algebra $\mathfrak{m}_0$ and also the first three Betti numbers of the finite-dimensional Lie algebras $\mathfrak{m}_0(n)$ defined as follows (1, 4):

$$\mathfrak{m}_0 = \mathrm{Span}(e_1, e_2, e_3, \dots), \quad [e_1, e_i] = e_{i+1}, \quad \text{for } i \geq 2,$$
$$\mathfrak{m}_0(n) = \mathrm{Span}(e_1, e_2, e_3, \dots, e_n), \quad [e_1, e_i] = e_{i+1}, \quad \text{for } 2 \leq i \leq n-1.$$

In the first few paragraphs, we closely follow the approach and the results of [7, Section 3], adapting them to the case of the ground field $\mathbb{Z}_2$. In effect, the outcome is that in the infinite-dimensional case, for $\mathfrak{g} = \mathfrak{m}_0$, the cohomology is "the same" as that for a field of characteristic zero, while in the finite-dimensional case, for $\mathfrak{g} = \mathfrak{m}_0(n)$, the situation is more delicate – not only the Betti numbers are different, but also the methods of [7, 1] and the very elegant approach of [2, Appendix B] do not work directly.

For a monomial $e^{i_1 i_2 \dots i_q} \in \Lambda^q(\mathfrak{g})$, $q \geq 1$, $i_1, i_2, \dots, i_q \geq 1$, (for both $\mathfrak{g} = \mathfrak{m}_0$ and $\mathfrak{g} = \mathfrak{m}_0(n)$) we have

$$\begin{aligned} d(e^{i_1 i_2 \dots i_q}) &= e^{1(i_1-1)i_2\dots i_q} + e^{1 i_1 (i_2-1)\dots i_q} + \dots + e^{1 i_1 i_2 \dots (i_q-1)} \\ &= e^1 \wedge \left(e^{(i_1-1)i_2\dots i_q} + e^{i_1(i_2-1)\dots i_q} + \dots + e^{i_1 i_2 \dots (i_q-1)}\right). \end{aligned} \tag{8}$$

It follows from (8) that the subspaces $\Lambda_k(\mathfrak{g})$ are d-invariant.

Moreover, for any $\omega \in \Lambda(\mathfrak{g})$ we have $d(e^1 \wedge \omega) = 0$ and $d(\omega) \in e^1 \wedge \Lambda(\mathfrak{g})$. Set $\mathfrak{h} := \mathrm{Span}(e_2, e_3, \dots)$ for $\mathfrak{m}_0$, and $\mathfrak{h} := \mathrm{Span}(e_2, e_3, \dots, e_n)$ for $\mathfrak{m}_0(n)$. Then $\mathfrak{h}$ is abelian and from (8) it follows that there is a well-defined linear operator D on $\Lambda(\mathfrak{h})$ such that for $\omega \in \Lambda(\mathfrak{h})$, we have

$$d\omega = e^1 \wedge (D\omega). \tag{9}$$

It is easy to see that

$$De^2 = 0, De^i = e^{i-1} \text{ for } i > 2, \quad D(\xi \wedge \eta) = D(\xi) \wedge \eta + \xi \wedge D(\eta) \text{ for } \xi, \eta \in \Lambda(\mathfrak{h}), \tag{10}$$

so D is a derivation of $\Lambda(\mathfrak{h})$. Recall that the *Lie derivative* with respect to e_1 is defined by taking the operator $(\mathrm{ad}_{e_1})^*$ on $\mathfrak{g}^*$ to be the dual to ad_{e_1} on $\mathfrak{g}$, and then extending it as a derivation to $\Lambda(\mathfrak{g})$. Note that D is just the restriction of $(\mathrm{ad}_{e_1})^*$ to $\Lambda(\mathfrak{h})$. Furthermore, $D(\Lambda^q_k(\mathfrak{h})) \subset \Lambda^q_{k-1}(\mathfrak{h})$, so that D is "nilpotent": for any $\omega \in \Lambda(\mathfrak{h})$ there exists $N = N(\omega) \geq 0$ such that $D^N \omega = 0$. For convenience, we define D^0 to be the identity map.

Since from (8), $\ker d = e^1 \wedge \Lambda(\mathfrak{h}) \oplus \ker D$, to find the kernel of d we need to find the kernel of D. This is given by the following lemma.

Lemma 3.1. (a) *Let* $\mathfrak{g} = \mathfrak{m}_0$. *For any* $\omega \in \Lambda(\mathfrak{h})$ *and* $e^i \in \mathfrak{h}$ *define*

$$F(\omega, e^i) = \sum_{l=0}^{\infty} D^l\omega \wedge e^{i+1+l} = \sum_{l=0}^{N(\omega)-1} D^l\omega \wedge e^{i+1+l}. \tag{11}$$

Then $F(\omega, e^i) \in \ker D$ *for* $\omega \wedge e^i = 0$ *and moreover, the elements*

$$\begin{gathered} F(e^{i_1 i_2 \dots i_q}, e^{i_q}) = e^{i_1 i_2 \dots i_q i_q+1} + De^{i_1 i_2 \dots i_q} \wedge e^{i_q+2} + \dots \in \Lambda_k^{q+1}(\mathfrak{h}), \\ \text{where } q \ge 1,\ 2 \le i_1 < i_2 < \dots < i_q,\ k = i_q + 1 + \sum_{j=1}^{q} i_j, \end{gathered} \tag{12}$$

form a basis for the kernel of the restriction of D *to* $\Lambda_k^{q+1}(\mathfrak{h})$*; the kernel of the restriction of* D *to* $\mathfrak{h}^*$ *is spanned by* e^2.

(b) *Let* $\mathfrak{g} = \mathfrak{m}_0(n)$, *viewed as the subspace of* $\mathfrak{m}_0$ *spanned by the first* n *vectors. Then* $\ker D$ *is the intersection of* $\ker D$ *constructed in* (a) *for the case* $\mathfrak{g} = \mathfrak{m}_0$ *with* $\mathfrak{m}_0(n)$.

Note that in the Introduction we used $D_1 = (\mathrm{ad}_{e_1})^*$ rather than D to define F. This yields the same object, since in (6), D only acts on elements of $\Lambda(\mathfrak{h})$ and D is the restriction on D_1 to $\Lambda(\mathfrak{h})$. Notice however that Lemma 3.1 concerns $\ker D$, which is different to $\ker D_1$.

Proof. (a) The fact that $F(\omega, e^i) \in \ker D$ follows immediately, as from (10), for any $\omega \in \Lambda(\mathfrak{h})$ and $e^i \in \mathfrak{h}$ we have

$$\begin{aligned} DF(\omega, e^i) &= D\Big(\sum_{l=0}^{\infty} D^l\omega \wedge e^{i+1+l}\Big) \\ &= \sum_{l=0}^{\infty} D^{l+1}\omega \wedge e^{i+1+l} + \sum_{l=0}^{\infty} D^l\omega \wedge e^{i+l} \\ &= \sum_{l=1}^{\infty} D^l\omega \wedge e^{i+l} + \sum_{l=0}^{\infty} D^l\omega \wedge e^{i+l} \\ &= \omega \wedge e^i, \end{aligned}$$

as we are working over $\mathbb{Z}_2$. Notice in passing that this also shows that D is surjective.

The fact that the elements given by (12) are linearly independent is also easy, as from among the monomials $e^{j_1 j_2 \dots j_q j_{q+1}}$, $2 \le j_1 < j_2 < \dots < j_q < j_{q+1}$ which appear on the right-hand side of the expansion of $F(e^{i_1 i_2 \dots i_q}, e^{i_q})$, there is exactly one with the property that $j_{q+1} = j_q + 1$, namely the monomial $e^{i_1 i_2 \dots i_q i_q+1}$. The fact that they indeed span the kernel of the restriction of D to $\Lambda_k^{q+1}(\mathfrak{h})$ follows from the same observation and from the dimension count. The elements $F(e^{i_1 i_2 \dots i_q}, e^{i_q}) \in \Lambda_k^{q+1}(\mathfrak{h})$ with $q \ge 1$, $2 \le i_1 < i_2 < \dots < i_q$, $i_q + 1 + \sum_{j=1}^{q} i_j = k$, are in one-to-one correspondence with the elements $e^{j_1 j_2 \dots j_q j_q+1} \in \Lambda_k^{q+1}(\mathfrak{h})$ with $2 \le j_1 < j_2 < \dots < j_q$. On the other hand, consider the linear operator $A : \Lambda_k^{q+1}(\mathfrak{h}) \to \Lambda_{k-1}^{q+1}(\mathfrak{h})$ defined on the monomials as follows: $Ae^{j_1 j_2 \dots j_q j_{q+1}} = e^{j_1 j_2 \dots j_q j_{q+1}-1}$. Then A is surjective and its kernel is spanned by the monomials $e^{j_1 j_2 \dots j_q j_q+1}$, so every surjective linear operator from $\Lambda_k^{q+1}(\mathfrak{h})$ to $\Lambda_{k-1}^{q+1}(\mathfrak{h})$ (in particular, D) has a kernel of the same dimension.

(b) easily follows from the fact that for the operator D defined for $\mathfrak{g} = \mathfrak{m}_0$, the subspace $\Lambda(\mathfrak{h})$ defined for $\mathfrak{m}_0(n)$ is D-invariant, and the restriction of D to it is the operator D defined for $\mathfrak{m}_0(n)$. ■

With Lemma 3.1 we can easily finish the computation of the cohomology for $\mathfrak{g} = \mathfrak{m}_0$; we obtain the same answer as in [7, Theorem 3.4]:

Theorem 3.2. *The cohomology classes of the cocycles*

$$e^1,\ e^2,\ F(e^{i_1 i_2 \dots i_q}, e^{i_q}), \tag{13}$$

where $q \geq 1,\ 2 \leq i_1 < i_2 < \ldots < i_q$, *form a basis for* $H^*(\mathfrak{m}_0)$ *over the field* $\mathbb{Z}_2$.

Furthermore, the dimensions of the homogeneous components of $H^*(\mathfrak{m}_0)$ over $\mathbb{Z}_2$ are the same as those over a field of characteristic zero, so in particular,

$$\dim H^q_{k+\frac{q(q+1)}{2}}(\mathfrak{m}_0) = P_q(k) - P_q(k-1),$$

where $P_q(k)$ is the number of partitions of a positive integer k into q parts. The products of the basis elements also have "the same" decomposition as in [7, Equation (8)], after reducing the coefficients modulo 2.

Proof of Theorem 3.2. From Lemma 3.1(a) we know $\ker D$, and so we know $\ker d = e^1 \wedge \Lambda(\mathfrak{h}) \oplus \ker D$. The image of d is just $e^1 \wedge \Lambda(\mathfrak{h})$, by (9) and from the surjectivity of D (which has been established in the proof of Lemma 3.1(a)). Putting these two facts together we get the claim. ■

We now turn our attention to the case $\mathfrak{g} = \mathfrak{m}_0(n)$. We view $\mathfrak{m}_0(n)$ as a subspace of $\mathfrak{m}_0$ spanned by the first n basis elements and for convenience, denote the operator D defined for $\mathfrak{m}_0$ by $\mathcal{D}$. The following Proposition easily follows from Lemma 3.1.

Proposition 3.3. *The space* $H^1(\mathfrak{m}_0(n))$ *is spanned by the classes of the elements* e^1, e^2 *and so* $b_1(\mathfrak{m}_0(n)) = 2$. *The space* $H^2(\mathfrak{m}_0(n))$ *is spanned by the classes of the elements* e^{1n}, $F(e^i, e^i) = e^{i,i+1} + e^{i-1,i+3} + \cdots + e^{2,2i-1}$, $2 \leq i \leq \frac{1}{2}(n+1)$, *and so* $b_2(\mathfrak{m}_0(n)) = \lfloor \frac{1}{2}(n+1) \rfloor$.

Proof. The claim for $H^1(\mathfrak{m}_0(n))$ is clear. For the second cohomology, by Lemma 3.1(a), the kernel of $\mathcal{D}$ is spanned by the elements $F(e^i, e^i) = e^{i,i+1} + e^{i-1,i+3} + \cdots + e^{2,2i-1}$. Since a sum of some number of the $F(e^i, e^i)$ belongs to $\mathfrak{m}_0(n)$ if and only if each of them does (no two monomials of the different $F(e^i, e^i)$ may possibly cancel), we get by Lemma 3.1(b):

$$\ker D = \mathrm{Span}(F(e^i, e^i)\ :\ 2 \leq i \leq \tfrac{1}{2}(n+1)). \tag{14}$$

Then $\ker d = e^1 \wedge \Lambda^1(\mathfrak{h}) \oplus \ker D$ and so the second coboundary space is spanned by $e^{1i}, F(e^i, e^i),\ i = 2, \ldots, n-1$. Then, as the image of d on the space of one-forms is spanned by $e^1 \wedge e^i$, for $1 \leq i \leq n-1$, the claim follows. ■

Proposition 3.3 establishes parts (a) and (b) of Theorem 1.2. The first two Betti numbers of $\mathfrak{m}_0(n)$ over $\mathbb{Z}_2$ are the same as those over a field of characteristic zero [1], but b_3 is different, as Theorem 1.2(c) shows.

Remark 3.4. Explicitly, for small values of n, Theorem 1.2(c) gives the values of $b_3(\mathfrak{m}_0(n))$ as in the second row of the following table.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
b_3	1	2	3	4	7	10	11	12	15	18	23	28	35	42	43	44	47	50

The sequence $b_3(\mathfrak{m}_0(n))$ is the sequence A266540 in [11][1]. To see that, we note that by the formula given in Theorem 1.2(c), $b_3(\mathfrak{m}_0(n)) = \frac{1}{2}(b_3(\mathfrak{m}_0(n-1)) + b_3(\mathfrak{m}_0(n+1)))$, for odd $n \geq 3$, and so it suffices to show that the even terms of the two sequences coincide, which is equivalent to the fact that the sequence $A_l := \frac{1}{2}b_3(\mathfrak{m}_0(2l)) = \frac{1}{3}(2^{2p-2}-1)+s^2$, where $l = 2^{p-1}+s$, $0 < s \leq 2^{p-1}$, coincides with A256249. This is equivalent to the fact that A_l is the $(l-1)$-st partial sum of the sequence A006257 given by $a_j = 2(j - 2^{\lfloor \log_2 j \rfloor}) + 1$. But the latter partial sum equals $l^2 - 1 - 2(2^{p-1}s + \sum_{i=0}^{p-2} 2^{2i})$, and the claim follows.

The proof of Theorem 1.2(c) is based on the following Proposition. Denote $W = \Lambda^3(e_2, \dots, e_{n-1})$ and $\mathfrak{h} = \mathrm{Span}(e_2, \dots, e_n)$.

Proposition 3.5. *For m as defined in Theorem 1.2, there exists $\omega_k \in W$ for $2 \leq k \leq m$ such that*

$$\ker D_{|\Lambda^3(\mathfrak{h})} = \ker D_{|W} \oplus \mathrm{Span}(e^n \wedge F(e^k, e^k) + \omega_k \,:\, 2 \leq k \leq m).$$

We first prove the theorem assuming the Proposition.

Proof of Theorem 1.2(c). For $n = 3$ the statement is easily verified, since $H^3(\mathfrak{m}_0(3))$ is spanned by the class of the single element e^{123}, so $b_1(\mathfrak{m}_0(3)) = 1$.

Assume $n \geq 4$. Denote d_n the dimension of the kernel of the operator D constructed for the algebra $\mathfrak{m}_0(n)$. Then from Proposition 3.5 we have $d_n = d_{n-1} + m - 1$. It follows that for $n = 2^p + m$, $0 < m \leq 2^p$, we have $d_n = d_{2^p} + \frac{1}{2}m(m-1)$ and in particular,

$$d_{2^{p+1}} = d_{2^p} + 2^{p-1}(2^p - 1). \tag{15}$$

We also have $d_4 = 1$, as for $\mathfrak{m}_0(4)$ the space $\ker D$ is spanned by e^{234}. It follows from (15) that $d_{2^p} = \frac{1}{3}(2^p-1)(2^{p-1}-1)$, and so $d_n = \frac{1}{3}(2^p-1)(2^{p-1}-1)+\frac{1}{2}m(m-1)$.

We have

$$\dim\ker(d\colon\Lambda^3(\mathfrak{m}_0(n))\to\Lambda^4(\mathfrak{m}_0(n))) = d_n+\dim(e^1\wedge\Lambda^2(\mathfrak{m}_0(n)) = d_n+\tfrac{1}{2}(n-1)(n-2).$$

On the other hand, from Proposition 3.3,

$$\dim\ker(d : \Lambda^2(\mathfrak{m}_0(n) \to \Lambda^3(\mathfrak{m}_0(n)) = (n-2) + \lfloor \tfrac{1}{2}(n+1) \rfloor,$$

and so the claim follows from (7). ■

Proof of Proposition 3.5. Any $\omega \in \Lambda^3(\mathfrak{h})$ can be uniquely represented as $\omega = e^n \wedge \xi + \omega'$, with $\xi \in \Lambda^2(e_2, \dots, e_{n-1})$, $\omega' \in \Lambda^3(e_2, \dots, e_{n-1}) = W$. For ω to belong to $\ker D$ it is necessary that $D\xi = 0$ (so that $D\omega$ does not contain e^n). From the proof of Proposition 3.3 it follows that ξ must be a linear combination of

[1] The authors are thankful to Omar E. Pol for pointing this out.

$F(e^k,e^k)$, $k=2,\dots,\lfloor n/2\rfloor$. Extracting the homogeneous components we obtain that the proposition is equivalent to the following statement: for $2\le k\le\lfloor n/2\rfloor$, there exists $\omega_k\in W$ such that $e^n\wedge F(e^k,e^k)+\omega_k\in\ker D$, if and only if $k\le m$.

The next step in the proof is the following lemma.

Lemma 3.6. *For $n\ge 4$ and $2\le k\le\lfloor n/2\rfloor$, define $a=\lceil(n+2k+1)/3\rceil$, $b=\lfloor n/2\rfloor+k-1$. There exists $\omega_k\in W$ such that $e^n\wedge F(e^k,e^k)+\omega_k\in\ker D$ if and only if the linear system $Ax=(1,0,\dots,0)^t\in\mathbb{Z}_2^{k-1}$ has a solution $x\in\mathbb{Z}_2^{b-a+1}$, where A is the $(k-1)\times(b-a+1)$-matrix given by*

$$A_{ij}=\binom{n-(a+j-1)+2(i-1)}{(a+j-1)+(i-1)-k}\mod 2,\qquad \begin{matrix}1\le i\le k-1,\\ 1\le j\le b-a+1,\end{matrix}\tag{16}$$

and as usual we set $\binom{N}{t}=0$ if $t<0$ or $t>N$.

Proof. Suppose for some $\omega_k\in W$, the three-form $\omega=e^n\wedge F(e^k,e^k)+\omega_k$ belongs to $\ker D$ (where $2\le k\le\lfloor n/2\rfloor$). Without loss of generality we can assume that ω_k is homogeneous, of the same degree as $e^n\wedge F(e^k,e^k)$, so that ω is homogeneous of degree $n+2k+1$.

By Lemma 3.1, the form ω viewed as a three-form on $\mathfrak{m}_0$, lies in the kernel of $\mathcal{D}$ and so is a linear combination of the forms $F(e^{s,r},e^r)$, $2\le s<r$, where by homogeneity we can assume that $s+2r+1=n+2k+1$, from which it follows that $s=n+2k-2r$. Then $2\le s\le r-1$ gives $a\le r\le b$. Therefore for some $\mu_r\in\mathbb{Z}_2$, $r=a,\dots,b$ we have

$$\begin{aligned}\omega&=F(e^k,e^k)\wedge e^n+\omega_k=\sum\nolimits_{r=a}^{b}\mu_rF(e^{n+2k-2r,r},e^r)\\&=\sum\nolimits_{r=a}^{b}\mu_r\sum\nolimits_{l=0}^{\infty}D^l(e^{n+2k-2r,r})\wedge e^{l+r+1}\\&=\sum\nolimits_{l=0}^{\infty}\sum\nolimits_{r=a}^{b}\mu_rD^l(e^{n+2k-2r,r})\wedge e^{l+r+1}.\end{aligned}\tag{17}$$

As $n+2k-2r=s<r\le b$ and $b=\lfloor n/2\rfloor+k-1\le 2\lfloor n/2\rfloor-1<n$, no terms $D^l(e^{n+2k-2r,r})$ in the latter expression may possibly contain e^N, $N\ge n$. It follows that the only terms containing e^N with $N\ge n$ in (17) are $\xi_N\wedge e^N$, where $\xi_N:=\sum_{r=a}^{\min\{b,N-1\}}\mu_rD^{N-r-1}(e^{n+2k-2r,r})$. In fact, since $\omega\in\Lambda^3(\mathfrak{m}_0(n))$, we have $\xi_N=0$ for all $N>n$ and equating the terms containing e^n we get $\xi_n=F(e^k,e^k)$. Conversely, if $\xi_n=F(e^k,e^k)$, then $\xi_N=0$ for all $N>n$, as $\xi_{n+1}=D\xi_n=DF(e^k,e^k)=0$, $\xi_{n+2}=D^2\xi_n=D^2F(e^k,e^k)=0$, and so on. Thus a necessary and sufficient condition for the existence of $\omega_k\in W$ such that the three-form $\omega=e^n\wedge F(e^k,e^k)+\omega_k$ belongs to $\ker D$ is the existence of $\mu_r\in\mathbb{Z}_2$, $r=a,\dots,b$ such that

$$F(e^k,e^k)=\xi_n=\sum\nolimits_{r=a}^{b}\mu_rD^{n-r-1}(e^{n+2k-2r,r}).\tag{18}$$

(the summation on the right-hand side is up to b as $b\le n-1$). Note that both sides are homogeneous two-forms of degree $2k+1$. Recall that $F(e^k,e^k)=e^{k,k+1}+e^{k-1,k+2}+\dots+e^{2,2k-1}$, and observe that

$$D^{n-r-1}(e^{n+2k-2r,r})=\sum\nolimits_{i=0}^{n-r-1}\binom{n-r-1}{i}e^{2k-r+i+1,r-i}.$$

So expanding and equating coefficients of the corresponding monomials we see that (18) is equivalent to the following system:

$$\begin{aligned}\sum\nolimits_{r=a}^{b} \mu_r\left(\tbinom{n-r-1}{r-k} + \tbinom{n-r-1}{r-(k+1)}\right) &= 1 \mod 2,\\ \sum\nolimits_{r=a}^{b} \mu_r\left(\tbinom{n-r-1}{r-(k-1)} + \tbinom{n-r-1}{r-(k+2)}\right) &= 1 \mod 2,\\ &\vdots\\ \sum\nolimits_{r=a}^{b} \mu_r\left(\tbinom{n-r-1}{r-2} + \tbinom{n-r-1}{r-(2k-1)}\right) &= 1 \mod 2.\end{aligned}$$

Now the linear combination of the first $s \le k-1$ of the above equations with the coefficients $\binom{2s-1}{s-1}, \binom{2s-1}{s-2}, \dots, \binom{2s-1}{1}, \binom{2s-1}{0}$ respectively gives

$$\sum\nolimits_{r=a}^{b} \mu_r\left(\sum\nolimits_{i=0}^{2s-1}\binom{2s-1}{i}\binom{n-r-1}{r-k-s+i}\right) = \sum\nolimits_{r=a}^{b} \mu_r\binom{n-r+2s-2}{r-k+s-1}$$

on the left-hand side (as $\sum_{i=0}^{l}\binom{l}{i}\binom{N}{t+i} = \sum_{i=0}^{l}\binom{l}{l-i}\binom{N}{t+i} = \binom{N+l}{t+l}$ by Vandermonde's identity). On the right-hand side we obtain $\binom{2s-1}{s-1}+\binom{2s-1}{s-2}+\dots+\binom{2s-1}{1}+\binom{2s-1}{0} = \frac{1}{2}\times 2^{2s-1} = 2^{2s-2}$, which is odd when $s=1$ and even otherwise. Thus the above system of equations is equivalent to the following one:

$$\sum\nolimits_{r=a}^{b} \mu_r\tbinom{n-r}{r-k} = 1 \mod 2, \quad \sum\nolimits_{r=a}^{b} \mu_r\tbinom{n-r+2s-2}{r-k+s-1} = 0 \mod 2, \text{ for } 2 \le s \le k-1.$$

This is equivalent to the claim of the lemma if we define $x = (\mu_a, \mu_{a+1}, \dots, \mu_b)^t$. ■

In order to use Lemma 3.6 to conclude the proof of the proposition, we need to show that the system $Ax = (1, 0, \dots, 0)^t$ has a solution if and only if $k \le m$. Even though we are working over $\mathbb{Z}_2$, let us say that vectors x, y are *orthogonal* if $x^t y = 0$.

To prove the **necessity** we show that, assuming $k > m$, the first row of A belongs to the span of the next $m-1$ rows, namely that

$$\left(\tbinom{k-m-1}{0}, \tbinom{k-m-1}{1}, \dots, \tbinom{k-m-1}{k-m-1}, 0, \dots, 0\right)A = 0 \mod 2. \tag{19}$$

Then any x orthogonal to all the rows of A starting from the second one, must also be orthogonal to the first row, and so the system $Ax = (1, 0, \dots, 0)^t$ has no solutions. To establish (19) we need to show that for every $j = 1, \dots, b-a+1$, we have

$$\sum\nolimits_{i=1}^{k-m}\binom{k-m-1}{i-1}\binom{n-(a+j-1)+2(i-1)}{(a+j-1)+(i-1)-k} = 0 \mod 2.$$

which is equivalent (by substitution $r = a+j-1$, $l = i-1$, $N = k-m-1$, $n = 2^p + m$) to showing that for all $r = a, \dots, b$,

$$\sum\nolimits_{l=0}^{N}\binom{N}{l}\binom{2^p-1-(r-k+N-2l)}{r-k+l} = 0 \mod 2. \tag{20}$$

We require the following Lemma.

Lemma 3.7. *Suppose $p \geq 2$ and let $x, y \in \mathbb{Z}$.*

(a) *If $0 \leq x < y < 2^p$, then $\binom{2^p+x}{y} = 0 \mod 2$.*

(b) *If $x, y \leq 2^p - 2$ and $y, x+y > 0$, then $\binom{2^p-1-x}{y} = \binom{y+x}{y} \mod 2$.*

Proof. By Kummer's Theorem, a binomial coefficient $\binom{q}{t}$ with $0 \leq t$ is odd if and only if there is a place in the binary representation where q has 0 and t has 1 and, when $0 \leq t \leq q$, if and only if there is a place in the binary representation where both $q - t$ and t have 1.

(a) For $\binom{2^p+x}{y} = 1 \mod 2$, the binary representation of $2^p + x$ must have a 1 at all the places where the binary representation of y does. But as $y < 2^p$, this implies that the binary representation of x has a 1 at all the places where the binary representation of y does, which contradicts the fact that $y > x$.

(b) First suppose $x \geq 0$. Then $\binom{2^p-1-x}{y}$ is even if and only if there is a place in the binary representation where $2^p - 1 - x$ has 0 and y has 1 if and only if there is a place in the binary representation where x has 1 and y has 1 if and only if $\binom{y+x}{y}$ is even.

Now let $x < 0$. So $\binom{y+x}{y} = 0$. Denote $z = -x - 1 \geq 0$. Then $\binom{2^p-1-x}{y} = \binom{2^p+z}{y}$ and $0 \leq z < y \leq 2^p - 2$ by our assumption. By part (a), $\binom{2^p+z}{y} = \binom{z}{y} \mod 2$, and $\binom{z}{y} = 0$ as $z < y$. So $\binom{y+x}{y} = \binom{2^p+z}{y} \mod 2$. ∎

To apply Lemma 3.7(b) to the binomial coefficients $\binom{2^p-1-(r-k+N-2l)}{r-k+l}$ from (20) we need to check few inequalities. We have $r - k \geq a - k = \lceil \frac{1}{3}(n-k+1) \rceil \geq \lceil \frac{1}{3}(n - \lfloor \frac{1}{2}n \rfloor + 1) \rceil = \lceil \frac{1}{3}(\lceil \frac{1}{2}n \rceil + 1) \rceil \geq 1$ and so $r - k + l \geq 1$ and $(r-k+l) + (r-k+N-2l) \geq 1$. Furthermore, $r-k+l, r-k+N-2l \leq r-k+N \leq b-k+N = \lfloor \frac{1}{2}n \rfloor + N - 1$, and $\lfloor \frac{1}{2}n \rfloor + N - 1 = \lfloor \frac{1}{2}n \rfloor + k - m - 2 \leq 2\lfloor \frac{1}{2}n \rfloor - m - 2 = 2\lfloor 2^{p-1} + \frac{1}{2}m \rfloor - m - 2 \leq 2^p - 2$. So the hypotheses of Lemma 3.7(b) are satisfied with $x = r-k+N-2l, y = r-k+l$. So Lemma 3.7(b) gives $\binom{2^p-1-(r-k+N-2l)}{r-k+l} = \binom{2(r-k)+N-l}{r-k+l} \mod 2$, for every $l = 0, \dots, N$. Vandermonde's identity gives $\binom{2(r-k)+N-l}{r-k+l} = \sum_{i=0}^{N-l} \binom{N-l}{i} \binom{2(r-k)}{r-k+l-i}$, and hence the left-hand side of (20) is congruent modulo 2 to

$$\begin{aligned}
\sum_{l=0}^{N} \binom{N}{l} \sum_{i=0}^{N-l} \binom{N-l}{i} \binom{2(r-k)}{r-k+l-i} &= \sum_{i,l \geq 0; i+l \leq N} \binom{N}{i, l, N-l-i} \binom{2(r-k)}{r-k+l-i} \\
&= \sum_{i > l \geq 0; i+l \leq N} \binom{N}{i, l, N-l-i} \left(\binom{2(r-k)}{r-k+l-i} + \binom{2(r-k)}{r-k+i-l} \right) \\
&\quad + \sum_{i \geq 0; 2i \leq N} \binom{N}{i, i, N-2i} \binom{2(r-k)}{r-k} \\
&= 0 \mod 2,
\end{aligned}$$

as $\binom{2(r-k)}{r-k+l-i} = \binom{2(r-k)}{r-k+i-l}$ and $\binom{2(r-k)}{r-k} = 2\binom{2(r-k)-1}{r-k}$. This completes the proof of necessity.

To prove the **sufficiency** we explicitly produce, for any $2 \le k \le m$, a vector $x \in \mathbb{Z}_2^{b-a+1}$ such that $Ax = (1, 0, \dots, 0)^t \in \mathbb{Z}_2^{k-1}$:

$$x_j = \sum_{s=0}^{p-1} \binom{m-k}{n-(a+j-1)-2^s}, \quad j = 1, \dots, b-a+1. \tag{21}$$

By Lemma 3.6 we need to show that for all $i = 1, \dots, k-1$,

$$\sum_{j=1}^{b-a+1} \left(\binom{n-(a+j-1)+2(i-1)}{(a+j-1)+(i-1)-k} \sum_{s=0}^{p-1} \binom{m-k}{n-(a+j-1)-2^s} \right) \bmod 2 = \delta_{1i}. \tag{22}$$

We first show that the expression on the left-hand side of (22) can be rewritten as

$$\sum_{s=0}^{p-1} \sum_{j\in\mathbb{Z}} \binom{n-(a+j-1)+2(i-1)}{(a+j-1)+(i-1)-k} \binom{m-k}{n-(a+j-1)-2^s} \quad \bmod 2,$$

so that there is no contribution from the values $j \le 0$ and $j \ge b-a+1$. The latter is easy: for the first binomial coefficient to be nonzero we need to have $n-(a+j-1)+2(i-1) \ge (a+j-1)+(i-1)-k$ which gives $2j \le n+k+i+1-2a \le n+2k-2a$, as $i \le k-1$, so $j \le \lfloor n/2 \rfloor + k - a = b-a+1$. To prove the former, we first look at the second binomial coefficient, from which we get $m-k \ge n-(a+j-1)-2^s$, so $j \ge n-a+1+k-m-2^s \ge n-\frac{1}{3}(n+2k+1)-\frac{2}{3}+1+k-m-2^s = \frac{1}{3}(2^{p+1}+k-m-3\cdot 2^s)$. Now if $s < p-1$ the expression on the right-hand side is positive, as $m \le 2^p$, and we are done. Suppose $s = p-1$. Then we have $j \ge \frac{1}{3}(2^{p-1}+k-m)$, which still implies $j > 0$ unless $m = 2^{p-1}+k+l$, $l \ge 0$, in which case we have $j \ge -\frac{1}{3}l$. Then

$$a = \left\lceil \frac{2^p+m+2k+1}{3} \right\rceil = \left\lceil \frac{2^p+2^{p-1}+3k+l+1}{3} \right\rceil = 2^{p-1}+k+\left\lceil \frac{l+1}{3} \right\rceil$$

and the first binomial coefficient has the form $\binom{2^p+x}{y}$, where

$$\begin{aligned} x &= n-(a+j-1)+2(i-1)-2^p = m-(a+j-1)+2(i-1) \\ &= 2^{p-1}+k+l-(a+j-1)+2(i-1) = l+1-\lceil (l+1)/3 \rceil + 2(i-1) - j, \\ y &= (a+j-1)+(i-1)-k = 2^{p-1}+\lceil (l+1)/3 \rceil + j + i - 2. \end{aligned}$$

Note that as $i \ge 1$, we have $x \ge 0$ if $j \le 0$. Also if $j \le 0$, then as $i \le k-1$, we have $y \le 2^{p-1}+\lceil (l+1)/3 \rceil + k - 3 \le 2^{p-1}+l+k-2 = m-2 < 2^p$. Moreover, if $j \le 0$, then as $i \le k-1$, we have $y-x = (2^{p-1}+\lceil (l+1)/3 \rceil + j+i-2) - (l+1-\lceil (l+1)/3 \rceil + 2(i-1) - j) = 2^{p-1}+2\lceil (l+1)/3 \rceil - (l+1)+2j-i \ge 2^{p-1}+2-(l+1)-k = 2^p-m+1 > 0$. So the hypotheses of Lemma 3.7(a) are satisfied, and hence the binomial coefficient $\binom{2^p+x}{y}$ is even. So it remains to establish that

$$\sum_{s=0}^{p-1} \sum_{j\in\mathbb{Z}} \binom{n-(a+j-1)+2(i-1)}{(a+j-1)+(i-1)-k} \binom{m-k}{n-(a+j-1)-2^s} \quad \bmod 2 = \delta_{1i}, \tag{23}$$

for all $i = 1, \dots, k-1$.

A clear advantage of (23) is that it "takes care of itself" – we do not have to worry about the limits. Changing the summation variable in (23) to $h = n - (a + j - 1) - 2^s$ we obtain that (23) is equivalent to

$$\sum_{s=0}^{p-1}\sum_{h\in\mathbb{Z}}\binom{2^s+2(i-1)+h}{n-2^s+(i-1)-k-h}\binom{m-k}{h} \mod 2 = \delta_{1i}. \tag{24}$$

Now for a polynomial $P \in \mathbb{Z}_2[t]$ and $l \in \mathbb{Z}$ we denote $\{P\}_l$ the coefficient of t^l in P. Consider the polynomial $P_{x,y}(t) = (t^2+t)^x(t^2+t+1)^y$. We have

$$P_{x,y}(t)=\sum_{h\in\mathbb{Z}}\binom{y}{h}(t^2+t)^{x+h}=\sum_{h,s\in\mathbb{Z}}\binom{y}{h}\binom{x+h}{s}t^{x+h+s}=\sum_{l\in\mathbb{Z}}\sum_{h\in\mathbb{Z}}\binom{x+h}{l-x-h}\binom{y}{h}t^l,$$

so the left-hand side of (24) equals

$$\begin{aligned}\sum_{s=0}^{p-1}\{P_{2^s+2(i-1),m-k}\}_{n+3(i-1)-k} &= \left\{\sum_{s=0}^{p-1}(t^2+t)^{2^s+2(i-1)}(t^2+t+1)^{m-k}\right\}_{n+3(i-1)-k}\\ &= \left\{\sum_{s=0}^{p-1}(t^2+t)^{2^s}(t^2+t)^{2(i-1)}(t^2+t+1)^{m-k}\right\}_{n+3(i-1)-k}\\ &= \{(t^{2^p}+t)(t^2+t)^{2(i-1)}(t^2+t+1)^{m-k}\}_{n+3(i-1)-k}\end{aligned}$$

modulo 2 (since as $(t^2+t)^{2^s} = t^{2^{s+1}} + t^{2^s}$ in $\mathbb{Z}_2[t]$ and so $\sum_{s=0}^{p-1}(t^2+t)^{2^s} = t^{2^{p+1}} + t \mod 2$). Now, if in the expansion of the latter polynomial we take t from the first parentheses, then the maximal degree of t in the resulting terms will be $1 + 4(i-1) + 2(m-k) \le 2m - 1 + 3(i-1) - k < n + 3(i-1) - k$, as $i \le k-1$ and $n = 2^p + m$, $m \le 2^p$. It follows that

$$\begin{aligned}\sum_{s=0}^{p-1}\{P_{2^s+2(i-1),m-k}\}_{n+3(i-1)-k} &= \{t^{2^p}(t^2+t)^{2(i-1)}(t^2+t+1)^{m-k}\}_{n+3(i-1)-k}\\ &= \{(t+1)^{2(i-1)}(t^2+t+1)^{m-k}\}_{m+(i-1)-k}\\ &= \sum_{l\in\mathbb{Z}}\{(t+1)^{2(i-1)}\}_{i-1+l}\{(t^2+t+1)^{m-k}\}_{m-k-l}\\ &= \{(t+1)^{2(i-1)}\}_{i-1}\{(t^2+t+1)^{m-k}\}_{m-k} \mod 2,\end{aligned}$$

where the last equality follows from the symmetry: for the polynomial $f(t) = (t+1)^{2(i-1)}$ we have $f(t) = t^{2(i-1)}f(t^{-1})$, so $\{(t+1)^{2(i-1)}\}_{i-1+l} = \{(t+1)^{2(i-1)}\}_{i-1-l}$, and similarly $\{(t^2+t+1)^{m-k}\}_{m-k-l} = \{(t^2+t+1)^{m-k}\}_{m-k+l}$.

Now if $i > 1$ we obtain $\{(t+1)^{2(i-1)}\}_{i-1} = \binom{2(i-1)}{i-1} = 0 \mod 2$, as required. If $i = 1$ we get $\{(t^2+t+1)^{m-k}\}_{m-k} = \{\sum_l \binom{m-k}{l}(t^2+t)^l\}_{m-k} = \{\sum_{l,h}\binom{m-k}{l}\binom{l}{h}t^{h+l}\}_{m-k} = \sum_l \binom{m-k}{l}\binom{l}{m-k-l} = \sum_s \binom{m-k}{s}\binom{m-k-s}{s}$, where $s = m - k - l$. The terms with $s < 0$ vanish, and the term with $s = 0$ is 1. For $s > 0$, consider the first place, counting from the right, where the binary expansion of s has a 1. Then by Kummer's Theorem, for $\binom{m-k}{s}$ to be nonzero, the binary expansion of $m-k$ must have a 1 at the same place, so the binary expansion of $m-k-s$ will have zero at that place, thus $\binom{m-k-s}{s} = 0$. It follows that $\{(t^2+t+1)^{m-k}\}_{m-k} = 1 \mod 2$, as required. This concludes the proof of Proposition 3.5 and hence of Theorem 1.2(c). ■

Note that one can extract from the above proof an explicit basis for the space of three-cocycles of $\mathfrak{m}_0(n)$ (and hence for $H^3(\mathfrak{m}_0(n))$). We have the following theorem.

Theorem 3.8. *For $n \geq 4$, $n = 2^p + m$, $0 < m \leq 2^p$ and for $2 \leq k \leq m$, define the numbers $a = \lceil (n+2k+1)/3 \rceil$, $b = \lfloor n/2 \rfloor + k - 1$. Let B_n be the set of elements of $\mathfrak{m}_0(n)$ of the form*

$$\sum_{r=a}^{b}\sum_{s=0}^{p-1}\binom{m-k}{n-r-2^s}F(e^{n+2k-2r,r}, e^r) = \sum_{r=a}^{b}\sum_{s=0}^{p-1}\binom{m-k}{n-r-2^s}\sum_{l\geq 0}D^l(e^{n+2k-2r}\wedge e^r)\wedge e^{r+l+1},$$

for $2 \leq k \leq m$, where D is the linear operator defined by (9) and the binomial coefficients are taken modulo 2. Then classes of the elements of the set

$$\{e^{1,i-1,i}, \quad 2+\lfloor n/2 \rfloor \leq i \leq n\} \cup \bigcup_{4\leq t\leq n} B_t.$$

is a basis for the cohomology space $H^3(\mathfrak{m}_0(n))$, $n \geq 4$, over the field $\mathbb{Z}_2$.

Proof. We start with the elements $e^{1,i-1,i}$, $2+\lfloor n/2 \rfloor \leq i \leq n$. They are linearly independent cocycles and the space spanned by them has the correct dimension, which is the codimension of the space of coboundaries in the space spanned by e^{1ij}, $1 < i < j \leq n$, by Proposition 3.3. It suffices to show that neither of them is a coboundary. But if it were so, then by homogeneity we would have had that $e^{1,i-1,i}$ is the coboundary of a linear combination of the elements e^{kl}, $2 \leq k < l \leq n$, $k+l = 2i$, that is, of the elements $e^{i-k,i+k}$, $k = 1,\ldots,n-i$ (note that as $i \geq 2+\lfloor n/2 \rfloor$, we have $2i-n-1 \geq 2$). But the coboundary of any such element is the sum of exactly two monomials, $e^{1,i-k-1,i+k} + e^{1,i-k,i+k-1}$, so the coboundary of any linear combination of them is a sum of an even number of monomials, hence cannot be equal to $e^{1,i-1,i}$.

As to the element from the sets B_t, no linear combination of them is a coboundary (as any coboundary is a multiple of e^1). Moreover, from Proposition 3.5 (both the statement and the proof) it follows that they form a basis for the kernel of D, where the form of the elements given in the statement follows from Lemma 3.6 and Equation (21). ■

Example 3.9. For $n = 4,\ldots,12$, the space of 3-cocycles of $\mathfrak{m}_0(n)$ is spanned by the three-forms e^{1ij}, $1 < i < j \leq n$, and the three-forms from the following table in the rows labelled by the numbers less than or equal to n.

4	e^{234}
5	
6	$e^{245}+e^{236}$
7	$e^{345}+e^{246}+e^{237},\ e^{356}+e^{257}+e^{347}$
8	$e^{256}+e^{247}+e^{238},\ e^{456}+e^{357}+e^{258}+e^{348}, e^{467}+e^{278}+e^{368}+e^{458}$
9	
10	$e^{267}+e^{258}+e^{249}+e^{23(10)}$
11	$e^{367}+e^{268}+e^{358}+e^{349}+e^{24(10)}+e^{23(11)}$, $e^{378}+e^{279}+e^{369}+e^{35(10)}+e^{25(11)}+e^{34(11)}$
12	$e^{467}+e^{368}+e^{458}+e^{269}+e^{25(10)}+e^{24(11)}+e^{23(12)}$, $e^{478}+e^{289}+e^{379}+e^{469}+e^{45(10)}+e^{35(11)}+e^{25(12)}+e^{34(12)}$, $e^{489}+e^{38(10)}+e^{47(10)}+e^{28(11)}+e^{46(11)}+e^{27(12)}+e^{36(12)}+e^{45(12)}$

4. Cohomology of $\mathfrak{m}_2$

In this section, we compute the cohomology of the infinite-dimensional Lie algebra $\mathfrak{m}_2$ given by (2):

$$\mathfrak{m}_2 = \mathrm{Span}(e_1, e_2, \dots), \qquad [e_1, e_i] = e_{i+1},\ i > 1, \quad [e_2, e_j] = e_{j+2},\ j > 2,$$

hence completing the proof of Theorem 1.1. First we state the following result for the truncation $\mathfrak{m}_2(n)$.

Corollary 4.1. *The first three Betti numbers of the Lie algebra $\mathfrak{m}_2(n)$, $n \ge 5$, over $\mathbb{Z}_2$ are given by $b_1(\mathfrak{m}_2(n)) = 2,\ b_2(\mathfrak{m}_2(n)) = [\frac{1}{2}(n+1)]$, and*

$$b_3(\mathfrak{m}_2(n)) = \tfrac{1}{3}(2^p - 1)(2^{p-1} - 1) + \tfrac{1}{2}m(m-1) + [\tfrac{1}{2}(n-1)],$$

where $n = 2^p + m,\ 0 < m \le 2^p$.

Proof. By [14, Theorem 1], the Betti numbers of $\mathfrak{m}_2(n)$ and of $\mathfrak{m}_0(n)$ over $\mathbb{Z}_2$ are the same. The claim then follows from Theorem 1.2. ■

Remark 4.2. It is easy to see that $H^1(\mathfrak{m}_2(n))$ is spanned by the cohomology classes of e^1 and e^2 and that $H^2(\mathfrak{m}_2(n))$ is spanned by the cohomology classes of the elements $e^{1n}+e^{2,n-1},\ e^{i,i+1}+e^{i-1,i+3}+\dots+e^{2,2i-1}$, where $2 \le i \le \frac{1}{2}(n+1)$. A basis for $H^3(\mathfrak{m}_2(n))$ can be found by applying the map f from [14, Definition 3] (see below) to the elements of the basis for $H^3(\mathfrak{m}_0(n))$ constructed in Theorem 3.8; the resulting basis is the same.

In the infinite-dimensional case, we follow the construction of [14]. As in the Introduction, let $V = \mathrm{Span}(e_1, e_2, \dots)$, and define the operator D_1 on V^* by $D_1 e^1 = D_1 e^2 = 0,\ D_1 e^i = e^{i-1}$, for $i > 2$, and then extend it to $\Lambda(V)$ as a derivation. Note that any $\omega \in \Lambda^q(V),\ q \ge 2$, has a unique presentation in the form $\omega = e^1 \wedge \xi + e^2 \wedge \eta + \zeta$, where $\xi \in \Lambda^{q-1}(e_2, e_3, \dots)$, $\eta \in \Lambda^{q-1}(e_3, e_4, \dots)$ and $\zeta \in \Lambda^q(e_3, e_4, \dots)$. Note that ξ, η and ζ linearly depend on ω.

Define the linear map f on $\Lambda(V)$ by setting $f(e^1 \wedge \xi + e^2 \wedge \eta + \zeta) = e^1 \wedge \xi + e^2 \wedge (\eta + D_1\xi) + \zeta$ on the forms of rank at least two, and taking it to be the identity on V^*. The following properties of f are easy to check:

- f is an involution, hence a bijection, and $f^{-1} = f$,
- the restriction of f to $\Lambda(e_2, e_3, \dots)$ is the identity,
- f preserves the homogeneous components: $f(\Lambda^q_k(V)) = \Lambda^q_k(V)$.

The main feature of f is the fact that it *interweaves* the differentials of $\mathfrak{m}_0$ and $\mathfrak{m}_2$. More precisely, consider $\mathfrak{m}_0$ and $\mathfrak{m}_2$ to have the same underlying linear space V, but to be defined by the brackets (1) and (2) respectively relative to the same basis $\{e_1, e_2, \dots\}$ for V. Then for all $\omega \in \Lambda(V)$, we have

$$f d_0 \omega = d_2 f \omega, \qquad f d_2 \omega = d_0 f \omega, \tag{25}$$

where d_0 and d_2 are the differentials on $\mathfrak{m}_0$ and $\mathfrak{m}_2$ respectively. The first equation is easily verified for $\omega = e^i$, and the proof for $\omega \in \Lambda^q(V)$, $q \geq 2$, is identical to the proof of [14, Proposition 1]. The second one follows, as f is an involution.

Proof of Theorem 1.1. By (25), f bijectively maps cocycles and coboundaries of $\mathfrak{m}_0$ to cocycles and coboundaries of $\mathfrak{m}_2$ respectively. It follows that $H^*(\mathfrak{m}_2)$ is spanned by the classes of the images under f of the elements (13). As f acts on all those elements as the identity, we obtain that the basis for $H^*(\mathfrak{m}_2)$ is the set of the classes of the same cocycles.

The fact that the multiplicative structure is preserved follows from the fact that the restriction of f to $\Lambda(e_2, e_3, \dots)$ is the identity and that multiplication by e^1 is trivial in both $H^*(\mathfrak{m}_0)$ and $H^*(\mathfrak{m}_2)$. Multiplication by e^1 is trivial in $H^*(\mathfrak{m}_0)$ because $e^1 \wedge \omega$ is a d_0-coboundary, for any ω (see the proof of Theorem 3.2). To see that multiplication by e^1 is trivial in $H^*(\mathfrak{m}_2)$, notice that for any ω in the list (13), one has $D\omega = 0$ (which is essentially assertion (a) of Lemma 3.1), and so $f(e^1 \wedge \omega) = e^1 \wedge \omega$, which is then a d_2-coboundary, as f maps coboundaries to coboundaries. ∎

Acknowledgement. This research would have never been done and this paper would have never been written without invaluable, incredibly generous contribution from Grant Cairns, at all the stages, from mathematics to presentation. We express to him our deepest gratitude.

References

[1] Armstrong, G., and S. Sigg, *On the cohomology of a class of nilpotent Lie algebras*, Bull. Austral. Math. Soc. **54** (1996), 517–527.

[2] Bordemann, M., *Nondegenerate invariant bilinear forms on nonassociative algebras*, Acta Math. Univ. Comenian. (N.S.) **66** (1997), 151–201.

[3] Cairns, G., and S. Jambor, *The cohomology of the Heisenberg Lie algebras over fields of finite characteristic*, Proc. Amer. Math. Soc. **136** (2008), 3803–3807.

[4] Caranti, A., S. Mattarei, and M. F. Newman, *Graded Lie algebras of maximal class*, Trans. Amer. Math. Soc. **349** (1997), 4021–4051.

[5] Caranti, A., and M. F. Newman, *Graded Lie algebras of maximal class. II*, J. Algebra **229** (2000), 750–784.

[6] Fialowski, A., *Classification of graded Lie algebras with two generators*, Mosc. Univ. Math. Bull. **38** (1983), 76–79.

[7] Fialowski, A., and D. Millionschikov, *Cohomology of graded Lie algebras of maximal class*, J. Algebra **296** (2006), 157–176.

[8] Gončarova, L. V., *Cohomology of Lie algebras of formal vector fields on the line*, Functional Anal. Appl. **7** (1973), 91–97.

[9] Jurman, G., *Graded Lie algebras of maximal class. III*, J. Algebra **284** (2005), 435–461.

[10] Millionschikov, D., *Graded filiform Lie algebras and symplectic nilmanifolds*, Geometry, topology, and mathematical physics, Amer. Math. Soc. Transl. Ser. 2, **212** (2004), 259–279.

[11] *The On-Line Encyclopedia of Integer Sequences*, published electronically at `http://oeis.org/`, 2016.

[12] Shalev, A., and E. Zelmanov, *Narrow Lie algebras: a coclass theory and a characterization of the Witt algebra*, J. Algebra **189** (1997), 294–331.

[13] Sköldberg, E., *The homology of Heisenberg Lie algebras over fields of characteristic two*, Math. Proc. R. Ir. Acad. **105A** (2005), 47–49.

[14] Tsartsaflis, I., *On the Betti numbers of filiform Lie algebras over fields of characteristic two*, Rev. Un. Mat. Argentina, to appear.

[15] Vergne, M., *Cohomologie des algèbres de Lie nilpotentes. Application à l'étude de la variété des algèbres de Lie nilpotentes*, Bull. Soc. Math. France **98** (1970), 81–116.

Yuri Nikolayevsky
Department of Mathematics
and Statistics
La Trobe University
Melbourne 3086, Australia
Y.Nikolayevsky@latrobe.edu.au

Ioannis Tsartsaflis
Department of Mathematics
and Statistics
La Trobe University
Melbourne 3086, Australia
itsartsaflis@students.latrobe.edu.au

Received January 30, 2016
and in final form October 9, 2016