Correction to
"On $BT_1$ group schemes and Fermat curves"

Rachel Pries and Douglas Ulmer

Abstract. We correct an error in Proposition 5.6(3) of [PU21] and revise other statements in the paper accordingly.

1. Corrected $u_{1,1}$-numbers

The calculation of $u_{1,1}$-numbers in part (3) of Proposition 5.6 in Section 5.3 of [PU21] is incorrect. In this section, we give more details on part (2) of Proposition 5.6 and a corrected statement and proof of part (3).

Before stating the result, we make the following definitions. Assume that $w$ is a primitive word of length $\lambda > 2$, and rotate $w$ so that it begins with $f$ and ends with $v$. Define $d(w)$ and $u(w)$ as follows: each subword of $w$ of the form $f^2(vf)^e v^2$ (where $e \geq 0$) contributes 1 to $d(w)$ and $e + 1$ to $u(w)$. Examples:

- $d(f^3 v^2) = 1, u(f^3 v^2) = 1, d(f^4 vf^2 v) = 0, u(f^4 vf^2 v) = 0$,
- $d(fv f^2 vf v^3) = 1, u(fv f^2 vf v^3) = 2$,
- $d(f^2 v^2 f^2 vf v^2) = 2, u(f^2 v^2 f^2 vf v^2) = 3$.

The invariant $d$ defined here turns out to be the same as the $u$ of Proposition 5.6. Also, as in Subsection 3.2, let $r$ be the integer such that (up to rotation) $w$ can be written in the form

$$w = v^{m_1} f^{m_2} \cdots v^{m_l} f^{m_l}$$

where all $m_i$ and $n_i$ are $\geq 1$.

The following replaces parts (2) and (3) of [PU21, Proposition 5.6].

Proposition. Let $w$ be a primitive word of length $\lambda > 2$.

1. There is a bijection

   $$\text{Hom}_{k\mathbb{Z}}(M(w), M_{1,1}) \cong k^{d(w)+r}.$$  

2. The $u_{1,1}$-number of $M(w)$ is $u(w)$.

Proof. For (1), we use Lemma 3.1 to present $M(w)$ with generators $E_0, \ldots, E_{\lambda-1}$ (with indices taken modulo $r$) and relations $V^n E_i = F^m E_{i-1}$. Let $z_0, z_1$ be a $k$-basis of $M_{1,1}$ with $Fz_0 = Vz_0 = z_1$ and $Fz_1 = Vz_1 = 0$. Then a homomorphism $\psi : M(w) \to M_{1,1}$ is determined by its values on the generators $E_i$. Write

   $$\psi(E_i) = a_{i,0} z_0 + a_{i,1} z_1.$$  

Received July 8, 2024.
Then $\psi$ is a $\mathbb{D}_k$-module homomorphism if and only if $V^{n_i}\psi(E_i) = F^{m_i}\psi(E_{i-1})$ for $i = 1, \ldots, r$.

This leads to the system of equations:

$$
\begin{align*}
\frac{a_{i,0}^{1/p}} & \quad \text{if } n_i = 1 \\
0 & \quad \text{if } n_i > 1
\end{align*}
$$

for $i \in \mathbb{Z}/r\mathbb{Z}$. Note that the $a_{i,1}$ are all unconstrained, and this accounts for the factor $k'$ on the right hand side of the display in part (1).

Since $w$ is primitive of length $> 2$, we may rotate $w$ so that $m_1 > 1$ or $n_r > 1$ (or both). First we deal with the case where all of the $m_i = 1$ and $n_r > 1$. The definitions above give $d(w) = u(w) = 0$ in this case. On the other hand, the system of equations for the $a_{i,0}$ reads

$$
\begin{align*}
0 &= a_{r-1,0}^p \\
\frac{a_{r-1,0}^{1/p}} & \quad \text{if } n_{r-1} = 1 \\
0 & \quad \text{if } n_{r-1} > 1
\end{align*}
$$

Clearly the only solution is $a_{0,0} = \cdots = a_{r-1,0} = 0$, and this shows that $\text{Hom}_{\mathbb{D}_k}(M(w), M_{1,1}) \cong k'$ and that none of these homomorphisms are surjective, in agreement with the calculations $d(w) = u(w) = 0$.

Now we assume that at least one of the $m_i > 1$, we rotate $w$ so that $m_1$ is one of them, and we write $1 = i_1 < i_2 < \cdots$ for the set of indices such that $m_{i_j} > 1$. Then the system (*) breaks up into subsystems involving the variables $a_{i_1,0}, \ldots, a_{i_j+1,0}$ and “controlled” by the subwords $s = v^{n_{i_j+1}} f \cdots v^n f^{m_{i_j}}$. (All the exponents of $f$ in this subword except $m_{i_j}$ are 1.) If none of the exponents of $v$ are $> 1$, then an argument similar to that in the previous paragraph shows that the only solution has $a_{i,0} = \cdots = a_{i_j+1,0} = 0$.

For the main case, continue to focus on a subword

$$s = v^{n_{i_1+1}} \cdots f^{m_{i_j}}$$

and assume that some exponent of $v$ in $s$ is $> 1$. To streamline notation, rewrite $s$ in the form

$$s = v^{n_1} \cdots f^{\mu_1} = (v f)^e v^{n_{i-1}} \cdots f^{\mu_1}$$

where $e \geq 0$ and we write $v.$ for $n_{i,j-1}$ and $\mu_1$ for $m_{i,j-1}$. Note that we have assumed that $\nu_{i-e} > 1$ and all $\mu_i = 1$ except $\mu_1$. Writing $a_i$ for $a_{m_i+1,0}$, the
relevant part of (\(*\)) reads

\[
\begin{align*}
\alpha_t^{1/p} &= \alpha_{t-1}^p \\
\alpha_{t-1}^{1/p} &= \alpha_{t-2}^p \\
& \vdots \\
\alpha_{m_t-e+1}^{1/p} &= \alpha_{t-e}^p \\
0 &= \alpha_{t-e-1}^p \\
\alpha_{t-e-1}^{1/p} &= \begin{cases} 
\alpha_{t-e-2}^p & \text{if } \nu_{t-e-1} = 1 \\
0 & \text{if } \nu_{t-e-1} > 1
\end{cases} \\
\alpha_{t-e-2}^{1/p} &= \begin{cases} 
\alpha_{t-e-3}^p & \text{if } \nu_{t-e-1} = 1 \\
0 & \text{if } \nu_{t-e-1} > 1
\end{cases} \\
& \vdots \\
\alpha_1^{1/p} &= \begin{cases} 
\alpha_{t-e}^p & \text{if } \nu_1 = 1 \\
0 & \text{if } \nu_1 > 1
\end{cases} \\
0 &= \alpha_{t-e-1}^p.
\end{align*}
\]

The general solution of this system is given by choosing \(a_t\) arbitrarily in \(k\) and letting

\[
a_t = a_{t-1}^{p^2} = \cdots = a_{t-e}^{p^e} \text{ and } a_{t-e-1} = \cdots = a_1 = 0. \quad (\ast\ast)
\]

This shows that there is one free parameter in the general solution of (\(*\)) for each subword \(s\) satisfying the hypotheses of this paragraph, and the general solution involves (a highly non-linear!) combination of \(e+1\) non-zero values.

To make the connection with the definitions of \(d(w)\) and \(u(w)\), note that the number of subwords of \(w = v^{n_1} \cdots f^{m_1}\) of the form \((vf)^e v^{n_2} \cdots f^{n_2}\) is the same as the number of subwords of the rotation \(f^{m_1} v^{n_1} \cdots v^{n_2}\) of the form \((vf)^e v^{n_2}\). Thus the general solution of (\(*\)) depends on exactly \(d(w) + r\) free parameters from \(k\). This completes the proof of part (1) of the proposition.

Turning to part (2), take an element \(\phi \in \operatorname{Hom}_{\mathcal{O}_k}(M(w), M_1^{\ast})\) for some integer \(u > 0\). The proof of part (1) gives explicit information about the matrix of \(\phi\) (as a \(k\)-linear map) with respect to a suitable basis which we now record. For an ordered basis of \(M(w)\), we take

\[
E_1, \ldots, E_r, FE_1, \ldots, FE_r, VE_1, \ldots, VE_r, ...
\]

where we omit \(VE_i\) if \(m_i = n_i = 1\) (since in this case this element has already appeared as \(FE_i\)) and the final \(\ldots\) stands for higher powers of \(F\) or \(V\) applied to the \(E_i\). As a basis of \(M_1^{\ast}\), we use \(u\) copies of \(z_0\) followed by \(u\) copies of \(z_1\).

Let \(A\) be the matrix of \(\phi\) with respect to these bases, and let \(A_0\) be the first \(u\) rows of \(A\). Then \(A_0\) is zero outside its first \(r\) columns, and its rows consist of zeroes and sequences \(a, a^{p^2}, a^{p^3}, \ldots, a^{p^{2e}}\) as described at (\(\ast\ast\)) above. In particular, only \(u(w)\) of the columns of \(A_0\) may be non-zero. This implies that \(u_{1,1}(M(w)) \leq u(w)\).
To see the reverse inequality, we choose solutions (**) so that $A_0$ has a block structure
\[
\begin{pmatrix}
0 & B_1 & 0 & 0 & \ldots \\
0 & 0 & 0 & B_2 & \ldots \\
\vdots & & & & \\
\end{pmatrix}
\]
where the $B_i$ correspond to the subwords $f^2(v f)^e v^2$ of $w$ and have the shape
\[
\begin{pmatrix}
\alpha_1 & \alpha_1^{p^2} & \alpha_1^{p^4} & \ldots & \alpha_1^{p^{2e}} \\
\alpha_2 & \alpha_2^{p^2} & \alpha_2^{p^4} & \ldots & \alpha_2^{p^{2e}} \\
\vdots & & & & \\
\alpha_{e+1} & \alpha_{e+1}^{p^2} & \alpha_{e+1}^{p^4} & \ldots & \alpha_{e+1}^{p^{2e}}
\end{pmatrix}
\]
Choosing the $\alpha_i \in k$ generically results in each of the $B_i$ having maximal rank, namely $e + 1$, and $A_0$ having rank $u(w)$.

With these choices of solutions of (****), the columns $r + 1, \ldots, 2r$ of the bottom half of $A$ (corresponding to the basis elements $FE_1, \ldots, FE_r$ and copies of $z_1$) has the shape
\[
\begin{pmatrix}
0 & B_1^{(p)} & 0 & 0 & \ldots \\
0 & 0 & 0 & B_2^{(p)} & \ldots \\
\vdots & & & & \\
\end{pmatrix}
\]
where $B^{(p)}$ is obtained from $B$ by taking the $p$-th power of each entry. It follows that $A$ has rank $2u(w)$, so our choices of solutions to (**) have produced a surjection $M(w) \rightarrow M_{u(w)}^{u_1,1}$, and this completes the proof that $u_{1,1}(M(w)) = u(w)$.

\[ \square \]

2. Other revisions

The correction to Proposition 5.6 requires minor revisions later in the paper:

- In Proposition 5.8 of [PU21], $u_{1,1}$ should be replaced by $\sum_w \mu_w d(w)$, where $H^1_{dR}(X) = \oplus_w M(w)^{\mu_w}$.
- In Proposition 5.9(4) of [PU21], the current formula for $u_{1,1}$ is
  \[
  \sum_{j=0}^{\lfloor (e-4)/2 \rfloor} \mu(-v^2(f v)^j f^2),
  \]
  and the correct formula is
  \[
  \sum_{j=0}^{\lfloor (e-4)/2 \rfloor} (j + 1) \mu(-f^2(v f)^j v^2).
  \]
- In the table of examples for $g = 4$ in Section 5.6 of [PU21], the $u_{1,1}$-number in the line $[0,0,1,1]$ should be 2.
In part (4) of Proposition 10.3 in [PU21], one should add a coefficient \((j + 1)\) to the summand in the display, so the correct formula is

\[
\sum_{j=0}^{\lfloor (\ell-4)/2 \rfloor} (j + 1) \left( \frac{p + 1}{2} \right)^2 \left( \frac{p - 1}{2} \right)^{2j+1} \left( \frac{p^{\ell-3-2j} - 1}{2} \right).
\]

Similarly, in part (4) of Proposition 11.3 in [PU21], the correct formula is

\[
\sum_{j=0}^{\lfloor (\lambda-4)/2 \rfloor} (j + 1) \left( \frac{p + 1}{2} \right)^2 \left( \frac{p - 1}{2} \right)^{2j+1} \left( \frac{p^{\lambda-3-2j} + 1}{2} \right)
\]

\[
+ \begin{cases} 
0 & \text{if } \lambda = 1, \\
\left( \frac{\lambda-1}{2} \right) \left( \frac{p+1}{2} \right)^2 \left( \frac{p-1}{2} \right)^{\lambda-2} & \text{if } \lambda > 1 \text{ and odd,} \\
\left( \frac{1}{2} \right) \left( \frac{p+1}{2} \right) \left( \frac{p-1}{2} \right)^{\lambda-1} & \text{if } \lambda \text{ even.}
\end{cases}
\]

References


Rachel Pries
Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA
pries@colostate.edu

Douglas Ulmer
Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA
ulmer@arizona.edu

This paper is available via http://nyjm.albany.edu/j/2024/30-45.html.