Characteristic and hyperinvariant subspaces over the field $GF(2)$

Pudji Astuti a, Harald K. Wimmer b,*

a Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Bandung 40132, Indonesia
b Mathematisches Institut, Universität Würzburg, Am Hubland, 97074 Würzburg, Germany

ARTICLE INFO

Article history:
Available online xxxx
Submitted by V. Mehrmann

AMS classification:
15A18
47A15
15A57

Keywords:
Hyperinvariant subspaces
Marked subspaces
Characteristic subspaces
Invariant subspaces
Jordan chains
Ulm sequence
Exponent
Height

ABSTRACT

Let $f$ be an endomorphism of a vector space $V$ over a field $K$. An $f$-invariant subspace $X \subseteq V$ is called hyperinvariant (respectively, characteristic) if $X$ is invariant under all endomorphisms (respectively, automorphisms) that commute with $f$. If $|K| > 2$ then all characteristic subspaces are hyperinvariant. If $|K| = 2$ then there are endomorphisms $f$ with invariant subspaces that are characteristic but not hyperinvariant. In this paper, we give a new proof of a theorem of Shoda, which provides a necessary and sufficient condition for the existence of characteristic non-hyperinvariant subspaces.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Let $V$ be an $n$-dimensional vector space over a field $K$ and let $f : V \rightarrow V$ be $K$-linear. The set of $f$-invariant subspaces of $V$ form a lattice, which we denote by $\text{Inv}(V)$. In this paper, we are concerned with two sublattices of $\text{Inv}(V)$. If a subspace $X$ of $V$ remains invariant for all endomorphisms of $V$ that commute with $f$ then $X$ is called hyperinvariant for $f$ [7, p. 305]. We say [2] that a subspace $X$ of $V$ is characteristic for $f$ if $X \in \text{Inv}(V)$ and $\alpha(X) = X$ for all $K$-automorphisms $\alpha$ of $V$ that commute with $f$. Let $\text{Hinv}(V)$ and $\text{Chinv}(V)$ be set of hyperinvariant and characteristic subspaces of $V$, respectively.

* Corresponding author. Fax: +49 931 8 88 46 11.
E-mail address: wimmer@mathematik.uni-wuerzburg.de (H.K. Wimmer)

0024-3795/$-$ see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2011.03.047

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field $GF(2)$, Linear Algebra Appl. (2011), doi:10.1016/j.laa.2011.03.047
Both sets are lattices, and $\text{Hinv}(V) \subseteq \text{Chinv}(V)$. If the characteristic polynomial of $f$ splits over $K$ (such that all eigenvalues of $f$ are in $K$) then one can reduce the study of $\text{Hinv}(V)$ and $\text{Chinv}(V)$ to the case where $f$ has only one eigenvalue, in particular to the case where $f$ is nilpotent. Thus, throughout this paper we shall assume $f^n = 0$. Then (see for example [7, p. 306]) the lattice $\text{Hinv}(V)$ is the smallest sublattice of $\text{Inv}(V)$ that contains

$$\text{Ker} f^k, \text{Im} f^k, \quad k = 0, 1, \ldots, n. \quad (1.1)$$

It is well known [10,12,2] that each characteristic subspace is hyperinvariant if $|K| > 2$. In this paper, we consider vector spaces $V$ over the field $K = \text{GF}(2)$ and we focus on characteristic subspaces that are not hyperinvariant. The following example shows that in the case of $K = \text{GF}(2)$ it may occur that $\text{Chinv}(V) \supsetneq \text{Hinv}(V)$. The set of endomorphisms, respectively, automorphisms, of $V$ that commute with $f$ will be denoted by $\text{End}_f(V)$, respectively, $\text{Aut}_f(V)$.

**Example 1.1.** Let $K = \text{GF}(2) = \{0, 1\}$. Consider $V = K^4$ and

$$f = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$ 

Let $e_1, \ldots, e_4$, be the unit vectors of $K^4$. Set $z = e_1 + e_3 = (1, 0, 1, 0)^T$. Then $f^2z = 0$. Define $X = \text{span}\{z, fz\}$. Then

$$X = \{0, z, fz, z + fz\} = \{0, e_1 + e_3, e_1 + e_3 + e_4\} \in \text{Inv}(V). \quad (1.2)$$

Note that $\text{End}_f(V)$ consists of all matrices of the form

$$g = \begin{pmatrix} a & b & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & d & c & 0 \\ k & h & d & c \end{pmatrix} \quad (1.3)$$

and $g \in \text{Aut}_f(V)$ if and only if

$$g = \begin{pmatrix} 1 & b & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & d & 1 & 0 \\ k & h & d & 1 \end{pmatrix}. \quad (1.4)$$

Thus, if $g \in \text{Aut}_f(V)$ then

$$gz = e_1 + e_3 + (k + d)e_4, \quad gfz = e_4, \quad g(z + fz) = e_1 + e_3 + (k + d + 1)e_4.$$ 

Hence $gX \subseteq X$, and therefore $X \in \text{Chinv}(V)$. Let $\pi_1 = \text{diag}(1, 0, 0, 0)$ be the orthogonal projection on $Ke_1$. Then $\pi_1 \in \text{End}_f(V)$, and we have $\pi_1z = e_1$, but $e_1 \notin X$. Therefore $X$ is not hyperinvariant.

The example is in accordance with the following result of Shoda [12, Satz 5, p. 619, 9,10, p. 63/64], which we state in terms of the Jordan normal form of $f$. 

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field $\text{GF}(2)$, Linear Algebra Appl. (2011), doi: 10.1016/j.laa.2011.03.047
Theorem 1.2. Let $V$ be a finite-dimensional vector space over the field $K = GF(2)$ and let $f : V \rightarrow V$ be nilpotent. The following statements are equivalent:

(i) There exists a characteristic subspace of $V$ which is not hyperinvariant.
(ii) For some numbers $r$ and $s$ with $s > r + 1$ the Jordan form of $f$ contains exactly one Jordan block of size $s$ and exactly one block of size $r$.

It is the main purpose of this paper to give a new proof of the implication “(i) $\Rightarrow$ (ii)” of Shoda’s theorem. In order to present a complete picture we also include a proof of the reverse implication “(ii) $\Rightarrow$ (i)”. Theorem 1.3 below plays a key role in our new proof. It relates characteristic and hyperinvariant subspaces with marked subspaces. Recall that an $f$-invariant subspace $W \subseteq V, W \neq 0$, is said to be marked [7, p. 83] if it has a Jordan basis (with respect to $f|_W$) that can be extended to a Jordan basis of $V$. The zero subspace is assumed to be marked.

Theorem 1.3 [2, p. 268]. Let $W \in \text{Inv}(V)$. Then $W$ is a hyperinvariant subspace if and only if $W$ is characteristic and marked.

The proof of Theorem 1.2 will be divided into several parts. It relies on results on characteristic subspaces in Section 4. Auxiliary material and basic facts on generator tuples and marked subspaces are discussed in Section 3.

2. Definitions and notation

We set $V[f^j] = \text{Ker} f^j, j \geq 0$. Clearly, $f^n = 0$ implies $V = V[f^n]$. Define $\iota = \text{id}_V$ and $f^0 = \iota$. Let $x \in V$. The smallest nonnegative integer $\ell$ with $f^\ell x = 0$ is called the exponent of $x$. We write $e(x) = \ell$. A nonzero vector $x$ is said to have height $q$ if $x \in f^q V$ and $x \notin f^{q+1} V$. In this case we write $h(x) = q$. We set $h(0) = \infty$. Let $Y \subseteq V$. We write $h(Y) = q$ if $h(y) = q$ for all $y \in Y$. Moreover, $h(Y) = q$ shall mean $Y \subseteq f^q V$ together with $Y \nsubseteq f^{q+1} V$. Let

$$
\langle x \rangle = \text{span}(f^i x, i \geq 0)
$$

be the cyclic subspace generated by $x$. If $B \subseteq V$ we define $\langle B \rangle = \sum_{b \in B} \langle b \rangle$. We call $U = (u_1, \ldots, u_k)$ a generator tuple of $V$ if

$$
V = \langle u_1 \rangle \oplus \cdots \oplus \langle u_k \rangle
$$

and if the elements of $U$ are ordered such that

$$
t_1 = e(u_1) \leq \cdots \leq e(u_k) = t_k.
$$

Let $\mathcal{U}$ be the set of generator tuples of $V$. Thus

$$
s^{t_1}, \ldots, s^{t_k}, \quad 0 < t_1 \leq \cdots \leq t_k
$$

are the elementary divisors of $f$, and $t_1 + \cdots + t_k = \dim V = n$ and $\dim \text{Ker} f = k$. Set

$$
N_\ell = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & \ddots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 1 & 0 \end{pmatrix}_{t \times t}.
$$

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field $GF(2)$, Linear Algebra Appl. (2011), doi:10.1016/j.laa.2011.03.047
Then \( J = \text{diag}(N_{t_1}, \ldots, N_{t_k}) \) is the Jordan form of \( f \). We define
\[
d(r) = \dim \left( \langle V[f] \cap f^{-1}V \rangle \cap f^rV \right), \quad r = 1, 2, \ldots, n.
\]
Using the terminology of abelian \( p \)-groups \([8]\) or \( p \)-modules \([10, \text{p.27}]\) we call \( d(r) \) the \( r - 1 \)th Ulm invariant and
\[
D = (d(1), \ldots, d(n)) \quad (2.4)
\]
the Ulm sequence of the pair \((V, f)\). Then \( d(r) \) is equal to the number of Jordan blocks of size \( r \) in the Jordan form \( J \) of \( f \). If \( V = \langle x \rangle \), \( e(x) = n \), then \( D = (0, \ldots, 0, 1) \). Thus, if \( V[f] = f^{a-1}V \) then \( D = (0, \ldots, 0, n/a, 0, \ldots, 0) \).

Let \( U = (u_1, \ldots, u_k) \in U \). It will be convenient to partition \( U \) into subsets of equal exponent. Denote the distinct elements of \( \{e(u_r); 1 \leq r \leq k\} \) by \( a_1, a_2, \ldots, a_m \) labeled so that \( a_1 < \cdots < a_m \) and set
\[
U_{a_\mu} = \{ u \in U; \ e(u) = a_\mu \}, \quad \mu = 1, \ldots, m.
\]
Then
\[
U = (U_{a_1}, \ldots, U_{a_m}) \quad \text{and} \quad e(U_{a_1}) = a_1 < \cdots < e(U_{a_m}) = a_m, \quad (2.5)
\]
and \( |U_{a_\mu}| = d(a_\mu) \). To (2.5) corresponds the decomposition
\[
V = \langle U_{a_1} \rangle \oplus \cdots \oplus \langle U_{a_m} \rangle. \quad (2.6)
\]
Let \( \pi_\mu : V \to V \) be the projection with
\[
\pi_\mu V = \langle U_{a_\mu} \rangle, \quad \text{Ker} \pi_\mu = \langle U_{a_1}, \ldots, U_{a_\mu-1}, U_{a_\mu+1}, \ldots, U_{a_m} \rangle.
\]
Note that \( \pi_\mu \in \text{End}_f(V) \).

3. Auxiliary results

3.1. Automorphisms and generators

The following lemma shows that each \( \alpha \in \text{Aut}_f(V) \) is uniquely determined by the image of a given generator tuple.

Lemma 3.1 [2]. Let \( U = (u_1, \ldots, u_k) \in U \) be given. For \( \alpha \in \text{Aut}_f(V) \) define \( \Theta_U(\alpha) = (\alpha(u_1), \ldots, \alpha(u_k)) \). Then
\[
\alpha \mapsto \Theta_U(\alpha), \quad \Theta_U : \text{Aut}_f(V) \to U.
\]
is a bijection.

The next lemma will enable us to exchange vectors in a generator tuple.

Lemma 3.2. Suppose \( V = \langle u_1 \rangle \oplus \cdots \oplus \langle u_n \rangle \) and \( e(u_i) = a, i = 1, \ldots, n \). If \( x \in V \), \( x \neq 0 \), and \( h(x) = 0 \), then there exist an index \( j \) such that
\[
(u_1, \ldots, u_{j-1}, x, u_{j+1}, \ldots, u_n) \in U. \quad (3.1)
\]
Proof. Let \( x = x_1 + \cdots + x_k, x_i \in \langle u_i \rangle \). Then
\[
x_i = \sum_{\nu=0}^{a-1} c_{i,\nu} f^\nu u_i = \left( u_i, f u_i, \ldots, f^{a-1} u_i \right) C_i
\]

Set
\[
C_i = \begin{pmatrix}
c_{i,0} & c_{i,1} & c_{i,2} & \cdots & c_{i,a-1} \\
c_{i,0} & c_{i,1} & c_{i,2} & \cdots & c_{i,a-1} \\
& c_{i,1} & c_{i,2} & \cdots & c_{i,a-1} \\
& & c_{i,1} & \cdots & c_{i,a-1} \\
& & & \cdots & \cdots \\
& & & & c_{i,a-1}
\end{pmatrix}
\]

Then
\[
\left( x_i, f x_i, \ldots, f^{a-1} x_i \right) = \left( u_i, f u_i, \ldots, f^{a-1} u_i \right) C_i
\]

and
\[
\left( x, f x, \ldots, f^{a-1} x \right) = \sum_{i=1}^{n} \left( u_i, f u_i, \ldots, f^{a-1} u_i \right) C_i.
\]

Because of \( h(x) = 0 \) we have \( h(x_i) = 0 \) for some \( j \). Thus \( c_{j,0} \neq 0 \), and \( C_j \) is nonsingular. We obtain
\[
\left( u_j, f u_j, \ldots, f^{a-1} u_j \right) = \left( x, f x, \ldots, f^{a-1} x \right) C_j^{-1} - \sum_{i \neq j} \left( u_i, f u_i, \ldots, f^{a-1} u_i \right) C_i C_j^{-1}.
\]

The vectors
\[
B = \left( u_1, f u_1, \ldots, f^{a-1} u_1, \ldots, u_k, f u_k, \ldots, f^{a-1} u_k \right)
\]

are a Jordan basis of \( V \). Because of \( (3.2) \) we obtain another Jordan basis if we replace the vectors \( \left( u_j, f u_j, \ldots, f^{a-1} u_j \right) \) in \( B \) by \( \left( x, f x, \ldots, f^{a-1} x \right) \). This proves \( (3.1) \). □

In the proof of Theorem 4.3 we shall use the following observation.

Lemma 3.3. Let \( U = (U_{a_1}, \ldots, U_{a_m}) \in \mathcal{U} \). Suppose \( i < j \) and let \( w \in U_{a_i}, y \in U_{a_j} \). Then there exists \( \alpha \in \text{Aut}_F(V) \) such that \( \alpha y = w + y \).

Proof. From \( y, w \in U \) follows \( h(y+w) = 0 \), and \( e(U_{a_i}) < e(U_{a_j}) \) implies \( h(f^{a_i-1} (y+w)) = a_i - 1 \) and \( e(y+w) = a_j \). We can assume \( U_{a_i} = (y, y_2, \ldots, y_r) \). Set \( \tilde{U}_{a_i} = (y+w, y_2, \ldots, y_r) \). If we replace \( U_{a_i} \) in \( U \) by \( \tilde{U}_{a_i} \) we obtain another generator tuple \( \tilde{U} \in \mathcal{U} \). Then Lemma 3.1 yields the desired automorphism. □

3.2. Marked subspaces

Marked subspaces can be traced back to [7, p. 83]. They have been studied in [4,6,1,5]. Let \( s^t_i, 0 < t_1 \leq \cdots \leq t_k \), be the elementary divisors of \( f \). We say that a \( k \)-tuple \( r = (r_1, \ldots, r_k) \) of integers is admissible if
\[
0 \leq r_i \leq t_i, \quad i = 1, \ldots, k.
\]

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field \( GF(2) \), Linear Algebra Appl. (2011), doi:10.1016/j.laa.2011.03.047
Each \( U \in \mathcal{U} \) together with an admissible tuple \( r \) gives rise to a subspace
\[
W(r, U) = \langle f^{r_1}u_1 \rangle \oplus \cdots \oplus \langle f^{r_k}u_k \rangle,
\]
which is marked in \( V \). Conversely, a subspace \( W \) is marked in \( V \) only if \( W = W(r, U) \) for some \( U \in \mathcal{U} \) and some admissible \( r \). The next theorem describes those subspaces \( W(r, U) \) that are independent of the generator tuple \( U \).

**Theorem 3.4** [21, p. 162]. Let \( U \in \mathcal{U} \) be given as in (2.1), and let \( r = (r_1, \ldots, r_k) \) be admissible. Then the following statements are equivalent:

(i) The subspace \( W(r, U) \) is characteristic.

(ii) The tuples \( t = (t_1, \ldots, t_k) \) and \( r = (r_1, \ldots, r_k) \) satisfy
\[
0 \leq t_1 \leq \cdots \leq r_k \quad \text{and} \quad t_1 - r_1 \leq \cdots \leq t_k - r_k.
\]

(iii) The subspace \( W(r, U) \) is hyperinvariant.

Note that (3.6) implies that \( r_i = r_j \) if \( t_i = t_j \). Let \( U = (U_{a_1}, \ldots, U_{a_m}) \), \( a_1 < a_2 < \cdots < a_m \). Hence if \( X \) is characteristic then \( X \) is marked if and only if
\[
X = f^{c_1}(U_{a_1}) \oplus \cdots \oplus f^{c_m}(U_{a_m})
\]
with \( 0 \leq c_i \leq a_i, i = 1, \ldots, m \) and
\[
c_1 \leq c_2 \leq \cdots \leq c_m, \quad \text{and} \quad a_1 - c_1 \leq a_2 - c_2 \leq \cdots \leq a_m - c_m.
\]
It is known that marked subspaces can be characterized in a basis free manner.

**Theorem 3.5** (see [1]). A subspace \( W \in \text{Inv}(V) \) is marked if and only if
\[
f^sW \cap f^{s+r}V = f^s(W \cap f^rV)
\]
for all \( s \geq 0, r \geq 0 \).

A different characterization of marked subspaces can be found in [6].

### 4. Characteristic subspaces

#### 4.1. Hyperinvariant subspaces and projections

Let \( U = (U_{a_1}, \ldots, U_{a_m}) \in \mathcal{U} \) be given as in (2.5) such that \( e(U_{a_\mu}) = a_\mu \), \( |U_{a_\mu}| = d(a_\mu), \mu = 1, \ldots, m \), and let (2.6), i.e. \( V = (U_{a_1}) \oplus \cdots \oplus (U_{a_m}) \), be the corresponding decomposition of \( V \). In the following we are concerned with characteristic subspaces \( X \) which have the property that \( x \in X \), implies
\[
\pi_i x \in X \quad \text{for all} \quad i = 1, \ldots, m.
\]
We have seen in Example 1.1 that (4.1) is not satisfied for all \( X \in \text{Chinv}(V) \).

**Lemma 4.1.** If \( X \) is a characteristic subspace of \( V \) then
\[
X \cap (U_{a_i}) = f^{c_i}(U_{a_i}), \quad i = 1, \ldots, m
\]
for some \( 0 \leq c_i \leq a_i \).

**Proof.** Let \( U_{a_1} = (v_1, \ldots, v_{c_1}). \) Set \( X_i = X \cap (U_{a_i}) \). Assume \( X_i \neq 0 \), and \( h(X_i) = c_i \). Then \( X_i \subseteq f^{c_i}(U_{a_i}) \).

Suppose \( y \in X_i \) and \( h(y) = c_i \). Then \( y = f^{c_i}w \) for some \( w \in V \) with \( h(w) = 0 \). We have \( w = w_1 + \cdots + w_m, w_j \in (U_{a_j}), j = 1, \ldots, m \). Then \( f^{c_i}w = f^{c_i}w_1 + \cdots + f^{c_i}w_m \in X_i \) and (2.6) imply
Let $X$ be a characteristic subspace of $V$. The following statements are equivalent:

- (i) $X$ is hyperinvariant.
- (ii) We have
  \[ X = (X \cap \langle U_{a_1} \rangle) \oplus \cdots \oplus (X \cap \langle U_{a_m} \rangle). \]  
  \[ (4.2) \]
- (iii) If $x \in X$, $x = x_1 + \cdots + x_m$, $x_i \in \langle U_{a_i} \rangle$, $i = 1, \ldots, m$, then
  \[ x_i \in X \quad \text{for all } i = 1, \ldots, m. \]  
  \[ (4.3) \]

Proof. (ii) $\iff$ (iii). Because of $X \cap \langle U_{a_i} \rangle \subseteq \pi_i X$ we have $\pi_i X \subseteq X$ if and only if
  \[ \pi_i X = X \cap \langle U_{a_i} \rangle. \]
  \[ (4.4) \]
It is obvious that (iii), as well as (ii), is satisfied if and only if (4.4) holds for all $i$, $i = 1, \ldots, m$.

(ii) $\implies$ (i) If (4.2) holds then Lemma 4.1 implies
  \[ X = f^{c_1} \langle U_{a_1} \rangle \oplus \cdots \oplus f^{c_m} \langle U_{a_m} \rangle. \]
Hence $X$ is marked, and it follows from Theorem 1.3 that $X$ is hyperinvariant. (i) $\implies$ (ii) Set $\bar{X} = \bigoplus_{i=1}^m (X \cap \langle U_{a_i} \rangle)$. Then $\bar{X} \subseteq X$. Let $x \in X$. Then $\pi_{\mu} x = x_{\mu} \in (X \cap \langle U_{a_i} \rangle)$, $\mu = 1, \ldots, m$. Hence $X \subseteq \bar{X}$. \[ \Box \]

We extend Lemma 4.2 to the case where $X \in \text{Chinv}(V) \setminus \text{Hinv}(V)$.

**Theorem 4.3.** If $X$ is a characteristic subspace then
  \[ \bar{X} = (X \cap \langle U_{a_1} \rangle) \oplus \cdots \oplus (X \cap \langle U_{a_m} \rangle) \]  
  \[ (4.5) \]
is the largest hyperinvariant subspace contained in $X$.

**Proof.** From Lemma 4.1 we obtain
  \[ X \cap \langle U_{a_i} \rangle = f^{c_i} \langle U_{a_i} \rangle, \quad 0 \leq c_i \leq a_i, \quad i = 1, \ldots, m. \]  
  \[ (4.6) \]
Hence
  \[ \bar{X} = f^{c_1} \langle U_{a_1} \rangle \oplus \cdots \oplus f^{c_m} \langle U_{a_m} \rangle. \]  
  \[ (4.7) \]
We show that $\bar{X}$ is hyperinvariant. By Theorem 3.4 we have to prove that $i < j$ implies
  \[ c_i \leq c_j \quad \text{and} \quad a_i - c_i \leq a_j - c_j. \]  
  \[ (4.8) \]
Suppose $i < j$ and let $v_i \in U_{a_i}$, $v_j \in U_{a_j}$. By Lemma 3.3 there exists an $\alpha \in \text{Aut}_f(V)$ such that $\alpha v_i = v_i + v_j$. Since $X$ is characteristic and $f^{c_i} v_j \in \bar{X} \subseteq X$ we have $\alpha (f^{c_i} v_j) = f^{c_i} (v_i + v_j) \in X$. Thus
  \[ f^{c_i} v_j \in f^{c_i} \langle U_{a_i} \rangle = X \cap \langle U_{a_i} \rangle \subseteq X \]
implies $f^{c_i} v_i \in X$. Hence $f^{c_i} v_i \in X \cap \langle U_{a_i} \rangle$. Then (4.6) yields $c_j \geq c_i$. 

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field $GF(2)$, Linear Algebra Appl. (2011), doi:10.1016/j.laa.2011.03.047
The second inequality in (4.8) can be proved as follows. Because of $e(v_i) = a_i = e(v_i + f^{a_j-a_i}v_j)$ we can substitute $v_i$ in $U_{a_i}$ by $v_i + f^{a_j-a_i}v_j$. Then there exists an $\alpha \in \text{Aut}_f(V)$ with $\alpha v_i = v_i + f^{a_j-a_i}v_j$. Hence

$$\alpha f^c v_i = f^c v_i + f^{c_i+a_j-a_i}v_j.$$  

Because of $f^{c_i}v_i \in X$ we have $f^{c_i}v_i + f^{c_i+a_j-a_i}v_j \in X$, and therefore $f^{c_i+a_j-a_i}v_j \in X$. Hence $f^{c_i+a_j-a_i}v_j \in \langle U_{a_i} \rangle$ implies $f^{c_i+a_j-a_i}v_j \in X \cap \langle U_{a_i} \rangle$. Then (4.6) yields $c_i + (a_j - a_i) \geq c_j$, i.e. $a_i - c_i \leq a_j - c_j$.

It remains to show that all hyperinvariant subspaces contained in $X$ are subsets of $\overline{X}$. Let $W \in \text{Hinv}(V)$. Then it follows from Lemma 4.2 that

$$W = (W \cap \langle U_{a_1} \rangle) \oplus \cdots \oplus (W \cap \langle U_{a_m} \rangle) = f^{d_1}\langle U_{a_1} \rangle \oplus \cdots \oplus f^{d_m}\langle U_{a_m} \rangle,$$

with suitable integers $0 \leq d_i \leq a_i$. Suppose $W \subseteq X$. Then

$$f^{d_i}\langle U_{a_i} \rangle = W \cap \langle U_{a_i} \rangle \subseteq X \cap \langle U_{a_i} \rangle = f^{c_i}\langle U_{a_i} \rangle.$$  

Therefore (4.7) implies $W \subseteq \overline{X}$. □

### 4.2. Special cases

In the following lemma we assume that $f$ is such that

$$d(a) = k > 1 \quad \text{and} \quad d(r) = 0 \quad \text{if} \quad r \neq a,$$

or equivalently $V[f] = f^{a-1}V$ and $\dim V[f] = k > 1$. In that case there are $k$ blocks in the Jordan form of $f$ and all Jordan blocks of $f$ have size $a$.

**Lemma 4.4.** Assume (4.9). Then there exist $\beta, \gamma \in \text{Aut}_f(V)$ such that $\beta + \gamma = \iota$.

**Proof.** Let $N_a$ be the Jordan block (2.3). Then the Jordan form of $f$ is

$$J = \text{diag}(N_a, \ldots, N_a) = I_k \otimes N_a,$$

and it is no loss of generality to assume $f = J$. Define $M = (N_a \otimes I_k) - (N_a^T \otimes I_k)$. Then

$$M = \begin{pmatrix} 0 & -I_k & 0 \\ I_k & 0 & -I_k \\ & & \ddots & \ddots \\ & & & \ddots \\ & & & & \ddots \\ & & & & & 0 & -I_k \\ & & & & & I_k & 0 \end{pmatrix}_{ak \times ak}$$

and $MJ = fM$. Set

$$P_1 = \text{diag}(1, 0, \ldots, 0)_{a \times a} \otimes I_k = \begin{pmatrix} I_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{ak \times ak},$$

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field $GF(2)$, Linear Algebra Appl. (2011), doi: 10.1016/j.laa.2011.03.047
\[ P_c = \text{diag}(0, 1, \ldots, 1)_{a \times a} \otimes I_k = \begin{pmatrix} 0 & & & 1 \\ & I_k & & \\ & & \ddots & \\ & & & I_k \end{pmatrix}_{ak \times ak}, \]

and \( \beta = M + P_1, \ \gamma = M + P_c. \) Then \( \beta, \gamma \in \text{Aut}_f(V), \) and \( \beta + \gamma = I. \) \( \square \)

**Lemma 4.5.** Suppose \( X \) is a characteristic subspace of \( V. \) Let \( x \in X \) and
\[
x = x_1 + \cdots + x_m, \quad x_i \in \langle U_{a_i} \rangle, \quad i = 1, \ldots, m.
\]
If \( |U_{a_i}| > 1 \) then \( x_s \in X. \)

**Proof.** According to Lemma 4.4 there exist \( \beta_s, \gamma_s \in \text{Aut}_f(\langle U_s \rangle) \) such that
\[
\beta_s + \gamma_s = \text{id}(U_s).
\]
Let \( \psi : V \to V \) and \( \phi : V \to V \) be given by
\[
\psi v = \phi v = v \quad \text{for } v \in \langle U_1, \ldots, U_{s-1}, U_{s+1}, \ldots, U_m \rangle
\]
and
\[
\psi v = \beta_s v, \quad \phi v = \gamma_s v \quad \text{for } v \in U_s.
\]
Then \( \psi, \phi \in \text{Aut}_f(V). \) Therefore \( (\psi + \phi)x = (\beta_s + \gamma_s)x_s = x_s \in X. \) \( \square \)

The following two theorems, which involve special types of Ulm sequences, will cover the hypothesis (i) of Theorem 5.1. It should be mentioned that the proofs of Theorems 4.6 and 4.8 below employ marked subspaces and thus are based on Theorem 1.3.

**Theorem 4.6.** If the sequence (2.4) contains at most one Ulm invariant with \( d(i) = 1, \) then each characteristic subspace of \( V \) is hyperinvariant.

**Proof.** Suppose \( |U_{a_1}| \geq 1, \) and \( |U_{a_i}| > 1 \) if \( i \neq q. \) Let \( x \in X \) and \( x = x_1 + \cdots + x_m, \) \( x_i \in \langle U_{a_i} \rangle, \quad i = 1, \ldots, m. \) Then Lemma 4.5 implies \( x_i \in X \) if \( i \neq q. \) Therefore, also \( x_q \in X, \) and we obtain (4.3). Then Lemma 4.2 completes the proof. \( \square \)

Bru et al. [4, Theorem 3.4, p. 223] have shown (see also [6, 3.2.4, p. 28]) that each invariant subspace of \( V \) is marked if and only if the sizes of blocks in the Jordan form of \( f \) differ at most by one. Then, for some \( q \) the space \( V \) is of the form \( V = \langle U_q \rangle \) or \( V = \langle U_q \rangle \oplus \langle U_{q+1} \rangle. \) We only need the special case where \( |U_q| = |U_{q+1}| = 1. \) Then \( f \) has Jordan form \( J = \text{diag}(N_q, N_{q+1}). \) For the sake of completeness we consider that case in a lemma and include a proof.

**Lemma 4.7.** Let
\[
V = \langle u_1 \rangle \oplus \langle u_2 \rangle \quad \text{and} \quad e(u_1) = q, \quad e(u_2) = q + 1.
\]
Then (i) each invariant subspace of \( V \) is marked, (ii) each characteristic subspace of \( V \) is hyperinvariant.

**Proof.** (i) Let \( W \in \text{Inv}(V), \ V \neq 0. \) Set \( h(W) = \min\{h(w) : w \in W, \ w \neq 0\}. \) It is easy to see that it suffices to consider subspaces \( W \) with \( h(W) = 0. \) Suppose \( W \) is cyclic, \( W = \langle w \rangle \) and \( h(w) = 0. \) Then \( e(w) = q \) or \( e(w) = q + 1. \) In the first case we have \( (w, u_2) \in \mathcal{U}, \) in the second case we obtain \( (u_1, w) \in \mathcal{U}. \) Thus \( \langle w \rangle \) is marked.

Now suppose \( W \) is not cyclic and \( h(W) = 0. \) Then \( W = \langle w_1 \rangle \oplus \langle w_2 \rangle, \) \( w_1 \neq 0, \) \( w_2 \neq 0, \) and \( \min\{h(w_1), h(w_2)\} = 0. \) Suppose \( h(w_1) = 0. \) If \( e(w_1) = q \) then we have \( (w_1, u_2) \in \mathcal{U}, \) and we can assume \( w_1 = u_1, \) such that \( W = \langle u_1 \rangle \oplus \langle w_2 \rangle. \) If \( w_2 = z_1 + z_2, z_i \in \langle u_i \rangle, i = 1, 2, \) then \( W = \langle u_1 \rangle \oplus \langle z_2 \rangle. \)
Lemma 4.9. Let \( h(z_2) = r \). Then \( z_2 = f^r v_2 \), where \( v_2 \in \langle u_2 \rangle \), \( h(v_2) = 0 \). Hence \( e(v_2) = q + 1 \) and \((u_1, v_2) \in \mathcal{U}\). Therefore \( W = \langle u_1 \rangle \oplus f^r \langle v_2 \rangle \). A similar argument works in the case \( e(w_1) = q + 1 \). (ii) This follows from Theorem 1.3. \( \square \)

Part (ii) of the preceding lemma is a special case of the following result.

**Theorem 4.8.** Suppose the Ulm sequence (2.4) contains exactly two invariants \( d(i) \) and \( d(j) \) equal to 1, and \( i \) and \( j \) are successive integers. Then each characteristic subspace \( X \subseteq V \) is hyperinvariant.

**Proof.** We can assume \( |U_{a_1}| = |U_{a_{m+1}}| = 1 \), \( a_1 = q \), \( a_{m+1} = q + 1 \), and \( |U_{a_1}| > 1 \) if \( a\_ \neq a_1 \) and \( a\_ \neq a_{m+1} \). Suppose \( X \subseteq V \) is characteristic. Let \( x \in X \) be decomposed as

\[
  x = x_1 + \cdots + x_{s-1} + (x_s + x_{s+1}) + x_{s+2} + \cdots + x_m, \tag{4.11}
\]

\( x_\mu \in \langle U_{a_\mu} \rangle \). Then Lemma 4.5 implies \( x_\mu \in X \) if \( \mu \neq s, \mu \neq s + 1 \). Hence \( x_s + x_{s+1} \in X \). Set \( X_\mu = X \cap \langle U_{a_\mu} \rangle \). Then

\[
  X = X_1 \oplus \cdots \oplus X_{s-1} \oplus (X \cap \langle U_{a_1}, U_{a_{m+1}} \rangle) \oplus X_{s+2} \oplus \cdots \oplus X_m. \tag{4.12}
\]

**Lemma 4.1** yields

\[
  X_\mu = f^\mu \langle U_{a_\mu} \rangle, \quad \text{if} \quad \mu \neq s, \mu \neq s + 1. \tag{4.13}
\]

Let \( \hat{f} \) be the restriction of \( f \) on \( \langle U_{a_1}, U_{a_{m+1}} \rangle \). We show that the subspace \( X_{s,s+1} := X \cap \langle U_{a_1}, U_{a_{m+1}} \rangle \) is characteristic in \( \langle U_{a_1}, U_{a_{m+1}} \rangle \) with respect to \( \hat{f} \). Let \( \hat{\alpha} \) be an automorphism of \( \langle U_{a_1}, U_{a_{m+1}} \rangle \) that commutes with \( \hat{f} \), and let \( \zeta_\mu, \mu = 1, \ldots, m \), be the identity map on \( \langle U_{a_\mu} \rangle \). We extend \( \hat{\alpha} \) in a natural way to an automorphism \( \alpha \) of \( V \) such that

\[
  \alpha = \zeta_1 + \cdots + \zeta_{s-1} + \hat{\alpha} + \zeta_{s+2} + \cdots + \zeta_m \in \text{Aut}(V). \tag{4.14}
\]

If \( x \in X_{s,s+1} \) then \( \hat{\alpha}x = \alpha x \in X \). Thus \( \hat{\alpha}x \in X_{s,s+1} \), which implies that \( X_{s,s+1} \) is characteristic in \( \langle U_{a_1}, U_{a_{m+1}} \rangle \) with respect to \( \hat{f} \). The pair \( \langle U_{a_1}, U_{a_{m+1}} \rangle \) is a generator tuple of \( \langle U_{a_1}, U_{a_{m+1}} \rangle \). From Lemma 4.7 we know that the characteristic subspace \( X_{s,s+1} \) is hyperinvariant and therefore marked in \( \langle U_s, U_{s+1} \rangle \). Hence

\[
  X \cap \langle U_s, U_{s+1} \rangle = X_{s,s+1} = f^{s} \langle U_s \rangle \oplus f^{s+1} \langle U_{s+1} \rangle. \tag{4.15}
\]

with \( \langle U_s, U_{s+1} \rangle = \langle U_s, U_{s+1} \rangle \). Combining (4.12) and (4.13) shows that \( X \) is marked. Therefore, by Theorem 1.3, the subspace \( X \) is hyperinvariant. \( \square \)

**4.3. Characteristic but not hyperinvariant**

Theorem 4.10 below is crucial for a proof of the implication “(ii) \( \Rightarrow \) (i)” of Theorem 1.2. We first note a technical lemma, which is adopted from [10, p. 63]. It clears the way for Theorem 4.10. Define

\[
  \langle U_{[i,j]} \rangle = \langle U_{a_i}, \ldots, U_{a_j} \rangle, \quad 1 \leq i \leq j \leq m. \tag{4.16}
\]

**Lemma 4.9.** Let \( U = \langle U_{a_1}, \ldots, U_{a_m} \rangle \in \mathcal{U} \), and

\[
  |U_{a_\rho}| = |U_{a_\tau}| = 1, \quad a_\rho + 1 < a_\tau. \tag{4.17}
\]

Let \( U_{a_\rho} = \langle u_{(\rho)} \rangle, U_{a_\tau} = \langle u_{(\tau)} \rangle \). Define

\[
  z = f^{-1} u_{(\rho)} + f^{a_\tau-1} u_{(\tau)} \tag{4.18}
\]

and

\[
  Y = \{ y \in V ; \ e(y) = 2, \ h(y) = a_\rho - 1, \ h(fy) = a_\tau - 1 \}. \tag{4.19}
\]

Please cite this article in press as: P. Astuti, H.K. Wimmer, Characteristic and hyperinvariant subspaces over the field \( GF(2) \), Linear Algebra Appl. (2011), doi:10.1016/j.laa.2011.03.047
Then $\langle Y \rangle$ is characteristic, and
\[ \langle Y \rangle = \langle z \rangle \oplus \langle \tilde{U}_{1\rho+1, \tau-1} \rangle[f] \oplus \langle \tilde{U}_{1\tau+1, m} \rangle[f^2]. \] \quad (4.17)

**Proof.** The subspace $\langle Y \rangle$ is defined via exponent and height. Hence it is characteristic. Set
\[ Q = \langle z \rangle \oplus \langle \tilde{U}_{1\rho+1, \tau-1} \rangle[f] \oplus \langle \tilde{U}_{1\tau+1, m} \rangle[f^2]. \]
We first show that $Y \subseteq Q$. Let $y \in Y$,
\[ y = x_1 + \cdots + x_m, \quad i = 1, \ldots, m. \]
Put $x_{[i,j]} = x_i + \cdots + x_j$, $1 \leq i \leq j \leq m$. From $h(y) = a_\rho - 1$ follows
\[ y \in \bigoplus_{i=1}^m f^{a_\rho-1} \langle u_i \rangle = \bigoplus_{i=1}^m f^{a_\rho-1} \langle U_i \rangle. \]
and $h(fy) = a_\tau - 1$ implies
\[ fy \in f^{a_\tau-1} \bigoplus_{i=\rho}^m \langle U_i \rangle = f^{a_\tau-1} \bigoplus_{i=\rho}^m \langle U_i \rangle. \]
Therefore $fx_i = 0$, $i = \rho, \ldots, \tau - 1$, and
\[ y \in f^{a_\rho-1} \langle u_\rho \rangle \oplus \langle \tilde{U}_{1\rho+1, \tau-1} \rangle[f] \oplus f^{a_\tau-2} \langle \tilde{U}_{1\tau, m} \rangle. \]
\[ (4.18) \]
From $e(y) = 2$ we obtain
\[ y \in f^{a_\rho-1} \langle u_\rho \rangle \oplus \langle \tilde{U}_{1\rho+1, \tau-1} \rangle[f] \oplus \langle \tilde{U}_{1\tau, m} \rangle[f^2]. \]
We have
\[ \langle \tilde{U}_{1\rho+1, \tau-1} \rangle[f] = \bigoplus_{i=\rho+1}^{\tau-1} f^{a_i-1} \langle U_i \rangle \subseteq f^{a_{\rho+1}-1} \bigoplus_{i=\rho+1}^{\tau-1} \langle U_i \rangle \subseteq f^{a_\rho} V. \]
The assumption $a_\tau > a_\rho + 1$ implies
\[ \langle \tilde{U}_{1\tau, m} \rangle[f^2] = \bigoplus_{i=\tau}^m f^{a_i-2} \langle U_i \rangle \subseteq \bigoplus_{i=\tau}^m f^{a_i-2} \langle U_i \rangle \subseteq f^{a_\rho} V \]
and
\[ \langle \tilde{U}_{1\tau+1, m} \rangle[f^2] \subseteq \bigoplus_{i=\tau+1}^m f^{a_{i-1}} \langle U_i \rangle \subseteq \bigoplus_{i=\tau+1}^m f^{a_i-1} \langle U_i \rangle. \]
\[ (4.19) \]
Hence (4.18) and $h(y) = a_\rho - 1$ yield $x_\rho \neq 0$, i.e. $x_\rho = f^{a_\rho-1} u_\rho$. Then
\[ y = f^{a_\rho-1} u_\rho + (x_{[\rho, \tau-1]} + (x_\tau + x_{[\tau+1, m]})) \]
\[ = x_{[\rho, \tau-1]} + x_{[\tau, m]} + x_{[\rho, \tau-1]} \in \langle \tilde{U}_{1\rho, \tau-1} \rangle[f], \quad x_{[\tau+1, m]} \in \langle \tilde{U}_{1\tau+1, m} \rangle[f^2]. \]
From $e(y) = 2$ and $fx_{[\rho, \tau-1]} = 0$ follows $x_{[\rho, \tau]} \neq 0$, $e(x_{[\tau, m]}) = 2$, and $fy = f(x_{[\tau, m]})$. Therefore $x_\tau \neq 0$. Otherwise $x_{[\tau+1, m]} \neq 0$, and then (4.19) would imply $h(fy) = h(fx_{[\tau+1, m]}) \geq a_\tau$. Hence
\[ x_\tau = f^{a_\tau-2} u_\tau + \gamma f^{a_\tau-1} u_\tau, \quad \gamma \in \{0, 1\}. \]
Putting the pieces together we obtain
\[ y = \left( f^{a_\rho-1} u_\rho + f^{a_\tau-2} u_\tau + \gamma f^{a_\tau-1} u_\tau \right) + x_{[\rho+1, \tau-1]} + x_{[\tau+1, m]}, \]
\[ (4.20) \]
and
\[ x_{[\rho+1, \tau-1]} \in \langle U_{1\rho, \tau-1} \rangle[f], \quad x_{[\tau+1, m]} \in \langle U_{1\tau+1, m} \rangle[f^2]. \]
\[ (4.21) \]
and

\[ f^{a_{\rho}}u_{(\rho)} + f^{a_{\tau}}u_{(\tau)} + \gamma f^{a_{\tau}}u_{(\tau)} = z + \gamma fz \in \langle z \rangle. \]

Hence \( y \in Q \) and \( \langle Y \rangle \subseteq Q \). The space \( Q \) is generated by vectors of the form

\[ z + x_{[\rho,1,\tau,1]} + x_{[\tau,1,m,l]}, \quad z + fx + x_{[\rho,1,\tau,1]} + x_{[\tau,1,m,l]}, \]

where \( x_{[\rho,1,\tau,1]} \) and \( x_{[\tau,1,m,l]} \) satisfy (4.21). It is easy to see that the vectors (4.22) lie in \( Y \). Hence \( Q \subseteq \langle Y \rangle \). □

In general, if (4.14) holds then there exists more than one characteristic subspace of \( V \) that is not hyperinvariant. In a subsequent paper [3] we construct a larger class of characteristic non-hyperinvariant subspaces of \( V \), which includes \( \langle Y \rangle \) as a special case.

Example 1.1 [continued.] If \( |K| = 2 \),

\[ V = K^4 = \langle e_1 \rangle \oplus \langle e_2 \rangle, \quad e(e_1) = 1, \quad e(e_2) = 3, \]

then (4.14) holds with \( (a_1,a_2) = (1,3) \). Let \( X \) be the subspace as in (1.2). Set \( z = e_1 + fe_2 = e_1 + e_3 \) and \( Y = \langle y; \quad e(y) = 2, \quad h(y) = 0, \quad h(fy) = 2 \rangle \). Then \( X = \langle z \rangle = \langle Y \rangle \).

If \( |K| > 2 \) then \( Y = \langle c_1e_1 + d_3e_2 + d_4e_4; \quad c_1 \neq 0, \quad d_3 \neq 0 \rangle \) and

\[ \langle Y \rangle = \text{span}\{e_1, e_3, e_4\} = \text{Ker}f^2. \]

Then \( Y \) is hyperinvariant, and \( \langle z \rangle \subsetneq \langle Y \rangle \).

Theorem 4.10. Suppose \( K = GF(2) \). Assume that (4.14) holds. Let

\[ Y = \{y; \quad e(y) = 2, \quad h(y) = a_\rho - 1, \quad h(fy) = a_\tau - 1\}. \]

Then the subspace \( \langle Y \rangle \) is characteristic and not hyperinvariant.

Proof. Let \( \pi_\rho : V \rightarrow V \) be the projection on \( \langle u_{(\rho)} \rangle \) along the complement \( \langle U_{a_1}, \ldots, U_{a_\rho-1}, U_{a_\rho+1}, \ldots, U_{a_m} \rangle \). Then \( \pi_\rho \) commutes with \( f \). If \( z \) is given by (4.15) then \( z \in \langle Y \rangle \) and \( \pi_\rho z = f^{a_{\rho}}u_{(\rho)} \). Note that \( f^{a_{\rho}}u_{(\rho)} \notin \langle z \rangle \). Therefore (4.17) implies \( \pi_\rho z \notin \langle Y \rangle \). Hence \( \langle Y \rangle \) is not hyperinvariant. □

5. Proof of Shoda’s theorem

We reformulate Theorem 1.2 in terms of Ulm invariants and thus make the connection with Theorem 26 of Kaplanski [10, p. 63].

Theorem 5.1 [12, 10]. Let \( K = GF(2) \) and \( f : V \rightarrow V \) be nilpotent. Then the following statements are equivalent:

(i) At most two Ulm invariants of \( (V, f) \) are equal to 1, and if there are exactly two, then they correspond to successive integers.

(ii) The characteristic subspaces of \( V \) are hyperinvariant.

Proof. Suppose condition (i) is satisfied. If there exists at most one Ulm invariant equal to 1 then we can apply Theorem 4.6. If there are exactly two Ulm invariants \( d(r) \) and \( d(s) \) equal to 1 and \( s = r + 1 \), then we can apply Theorem 4.8. If condition (i) is not satisfied then we have (4.14) for some \( \rho, \tau \). Thus Theorem 4.10 completes the proof. □
Acknowledgment

We are indebted to referees for valuable comments and suggestions.

References