GENERALIZED $F$-SIGNATURE OF INVARIANT SUBRINGS

MITSUYASU HASHIMOTO AND YUSUKE NAKAJIMA

ABSTRACT. It is known that a certain invariant subring $R$ has finite $F$-representation type. Thus, we can write the $R$-module $\varepsilon R$ as a finite direct sum of finitely many $R$-modules. In such a decomposition of $\varepsilon R$, we pay attention to the multiplicity of each direct summand. For the multiplicity of free direct summand, there is the notion of $F$-signature defined by C. Huneke and G. Leuschke and it characterizes some singularities. In this paper, we extend this notion to non-free direct summands and determine the explicit values of them.

1. INTRODUCTION

Throughout this paper, we suppose that $k$ is an algebraically closed field of prime characteristic $p > 0$, and $V$ is a $d$-dimensional $k$-vector space. Let $G \subset \text{GL}(V)$ be a finite subgroup such that the order of $G$ is not divisible by $p$, and $G$ contains no pseudo-reflections. Let $S$ be a symmetric algebra of $V$. We denote the invariant subring of $S$ under the action of $G$ by $R := S^G$. Sometimes we denote $p^e$ by $q$. Since $\text{char}R = p > 0$, we can define the Frobenius map $F : R \to R (r \mapsto r^p)$ and also define the $e$-times iterated Frobenius map $F^e : R \to R (r \mapsto r^{p^e})$ for $e \in \mathbb{N}$. For any $R$-module $M$, we denote the module $M$ with its $R$-module structure pulled back via $F^e$ by $\varepsilon M$. That is, $\varepsilon M$ is just $M$ as an abelian group, and its $R$-module structure is given by $r \cdot m := F^e(r)m = r^{p^e}m$ for all $r \in R$, $m \in M$.

In our assumption, it is known that the invariant subring $R$ has finite $F$-representation type (or FFRT for short). The notion of FFRT is defined by K. Smith and M. Van den Bergh [SVdB].

Definition 1.1. We say that $R$ has finite $F$-representation type by $\mathcal{N}$ if there is a finite set $\mathcal{N}$ of isomorphism classes of finitely generated $R$-modules, such that for any $e \in \mathbb{N}$, the $R$-module $\varepsilon R$ is isomorphic to a finite direct sum of elements of $\mathcal{N}$.

More explicitly, finitely many finitely generated $R$-modules which form such a finite set $\mathcal{N}$ are described as follows.

Proposition 1.2 ([SVdB]). Let $V_0 = k, V_1, \cdots, V_n$ be a complete set of non-isomorphic irreducible representations of $G$ and we set $M_i := (S \otimes_k V_i)^G$ ($i = 0, 1, \cdots, n$). Then $R$ has FFRT by $\{M_0 \cong R, M_1, \cdots, M_n\}$.

From this proposition, we can decompose $\varepsilon R$ as follows

$$\varepsilon R \cong R^{\oplus c_{0,e}} \oplus M_1^{\oplus c_{1,e}} \oplus \cdots \oplus M_n^{\oplus c_{n,e}}.$$

Now, we want to investigate the multiplicities $c_{i,e}$. For the multiplicity of the free direct summand, that is, for the multiplicity $c_{0,e}$, there is the notion of $F$-signature defined by C. Huneke and G. Leuschke.

2010 Mathematics Subject Classification. Primary 13A35, 13A50.

Key words and phrases. $F$-signature, finite $F$-representation type, invariant subrings.
Definition 1.3 ([HL]). The $F$-signature of $R$ is $s(R) := \lim_{e \to \infty} \frac{c_{0,e}}{p^de}$, if it exists.

Note that K. Tucker showed its existence under more general settings [Tuc] (see also Proposition 3.1). And it is known that this numerical invariant characterizes some singularities. For example, $s(R) = 1$ if and only if $R$ is regular [HL] (see also [Yao2]), and $s(R) > 0$ if and only if $R$ is strongly $F$-regular [AL]. In our situation, the $F$-signature of the invariant subring $R$ is determined as follows and it implies that $R$ is strongly $F$-regular.

Theorem 1.4 ([WY]). The $F$-signature of the invariant subring $R$ is

$$s(R) = \frac{1}{|G|}.$$

Remark 1.5. In [WY], this theorem is proved in terms of minimal relative Hilbert-Kunz multiplicity. And Y. Yao showed that it coincides with the $F$-signature [Yao2].

Now, we extend this notion to other direct summands. Namely, we investigate the multiplicities $c_{i,e} (i = 1, \cdots, n)$ and determine the limit $\lim_{e \to \infty} \frac{c_{i,e}}{p^d e}$. In order to determine this limit, we have to care about the next two problems first.

- For each $e \in \mathbb{N}$, are the multiplicities $c_{i,e}$ determined uniquely?
- Does the limit $\lim_{e \to \infty} \frac{c_{i,e}}{p^d e}$ exist?

In Section 2, we will show the uniqueness of the multiplicities. In Section 3, we will show the existence of the limit and determine the limit.

Acknowledgment. The authors would like to thank Professor Kei-ichi Watanabe for valuable advice and also thank Professor Peter Symonds for reading the previous version of this manuscript and pointing out that the Brauer character is more suitable to prove the main theorem.

2. Uniqueness of decomposition

In this section, we show the uniqueness of the multiplicities. Firstly, we introduce the notion of Frobenius twist (e.g. [Jan]).

Definition 2.1. For $k$-vector space $V$ and $e \in \mathbb{Z}$, we define $k$-vector space $^eV$ as follows

- $^eV$ is the same as $V$ as an additive group;
- the action of $\alpha \in k$ on $^eV$ is $\alpha \cdot v = \alpha^e v$.

An element $v \in V$, viewed as an element of $^eV$, is sometimes denoted by $^e v$. Thus $\alpha \cdot ^e v = \epsilon(\alpha^e v)$. By the composition $G \hookrightarrow \text{GL}(V) \xrightarrow{\phi} \text{GL}(^eV)$, $^eV$ is also a representation of $G$, where $\phi$ is given by $\phi(g)(^e v) = \epsilon(g v)$ for $g \in G$ and $v \in V$. We call this representation the Frobenius twist of $V$. Sometimes we denote this representation by $V(-e)$.

Let $v_1, \cdots, v_d$ be a basis of $V$. For this basis, we suppose that a representation of $G$ is defined by

$$g \cdot v_j = \sum_{i=1}^d f_{ij}(g)v_i \quad (g \in G, \ f_{ij} : G \to k).$$
Namely, a matrix representation of $V$ is described by $(f_{ij}(g))$. Since $k$ is an algebraically closed field, the basis $v_1, \ldots, v_d$ also form a basis of $\mathcal{E}V$, and the action of $G$ on $\mathcal{E}V$ is described as follows

$$g \cdot \mathcal{E}v_j = \mathcal{E}(g \cdot v_j) = \mathcal{E}(\sum_{i=1}^{d} f_{ij}(g)v_i) = \sum_{i=1}^{d} f_{ij}(g)^{p^e}(\mathcal{E}v_i).$$

From this observation, a matrix representation of the Frobenius twist $\mathcal{E}V$ is described by $((f_{ij}(g))^{p^e})$, that is, each component of the matrix representation of $\mathcal{E}V$ is the $p^{-e}$-th power of the original one.

In order to show the uniqueness of the multiplicities, we prove the following.

**Proposition 2.2.** For $e \geq 1$, $c_{0,e}, \ldots, c_{n,e} \geq 0$, the following decompositions are equivalent

1. $\mathcal{E}R \cong M_0^{c_{0,e}} \oplus M_1^{c_{1,e}} \oplus \cdots \oplus M_n^{c_{n,e}}$ as $R$-modules;
2. $\mathcal{E}S \cong (S \otimes_k V_0)^{c_{0,e}} \oplus (S \otimes_k V_1)^{c_{1,e}} \oplus \cdots \oplus (S \otimes_k V_n)^{c_{n,e}}$ as $(G,S)$-modules;
3. $\mathcal{E}S/m^eS \cong V_0^{c_{0,e}} \oplus V_1^{c_{1,e}} \oplus \cdots \oplus V_n^{c_{n,e}}$ as $G$-modules;
4. there exist $\alpha_{ij} \in \frac{1}{q}Z_{\geq 0}$ such that $\mathcal{E}S \cong \bigoplus_{i=0}^{n} \bigoplus_{j=1}^{c_{i,e}} (S \otimes_k V_i)(-\alpha_{ij})$ as $\frac{1}{q}Z$-graded $(G,S)$-modules;
5. there exist $\alpha_{ij} \in \frac{1}{q}Z_{\geq 0}$ such that $\mathcal{E}R \cong \bigoplus_{i=0}^{n} \bigoplus_{j=1}^{c_{i,e}} M_i(-\alpha_{ij})$ as $\frac{1}{q}Z$-graded $R$-modules.

In order to prove this proposition, the next theorem plays the central role.

**Theorem 2.3** ([Has]). If $G$ contains no pseudo-reflections, then the functor $\text{Ref}(G,S) \to \text{Ref}(R)$ ($M \mapsto M^G$) is an equivalence, where $\text{Ref}(G,S)$ is the category of reflexive $(G,S)$-modules and $\text{Ref}(R)$ is the category of reflexive $R$-modules. The quasi-inverse is $N \mapsto (S \otimes_R N)^{**}$.

The same functors give an equivalence $^*\text{Ref}(G,S) \to ^*\text{Ref}(R)$, where $^*\text{Ref}(G,S)$ is the category of $\mathbb{Z}[1/p]$-graded reflexive $(G,S)$-modules and $^*\text{Ref}(R)$ is the category of $\mathbb{Z}[1/p]$-graded reflexive $R$-modules.

**Proof of Proposition 2.2.** The equivalence of (1) and (2), (4) and (5) are obtained by Theorem 2.3, and (3) is obtained by applying $(\otimes_S k)$ to (2). If we forget the grading from (4), then we obtain (2).

\[
\begin{array}{ccc}
(1) & \overset{\text{Thm.2.3}}{\iff} & (2) \\
(3) & \overset{\text{forget grading}}{\iff} & (4) \\
(5) & \overset{\text{Thm.2.3}}{\iff} &
\end{array}
\]

So we may show (3) $\Rightarrow$ (4). If we consider $\mathcal{E}S/m^eS$ as $\frac{1}{q}Z$-graded $G$-modules, then we can write

$$\mathcal{E}S/m^eS \cong \bigoplus_{i=0}^{n} \bigoplus_{j=1}^{c_{i,e}} V_i(-\alpha_{ij}).$$

If we consider $\mathcal{E}S/m^eS$ as $G$-modules, then $\mathcal{E}S \cong S \otimes_k (\mathcal{E}S/m^eS)$ (cf. [SVdB, proof of Proposition 3.2.1]). So we obtain the description (4). \qed
Especially, the decomposition (3) appears in Proposition 2.2 is unique. Thus, we obtain the next statement as a corollary.

**Corollary 2.4.** Each $M_i$ is indecomposable and the multiplicities $c_{i,e}$ are determined uniquely.

In Proposition 2.2 and Corollary 2.4, the condition “$G$ contains no pseudo-reflections” is essential. If $G$ contains a pseudo-reflection, then there is a counter-example as follows.

**Example 2.5.** Let $S = k[x,y]$ be a polynomial ring, where $(\text{char } k, |G|) = 1$. Set $G = \langle \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$, that is $G$ is a symmetric group $\mathbb{Z}_2$, and $V_0 = k, V_1 = \text{sgn}$ are irreducible representations of $G$. (Note that $\sigma$ is a pseudo-reflection.) Then, $R := S^G \cong k[x+y,xy]$. Since $R$ is a polynomial ring, $eR \cong R^{pde}$. On the other hand,

$$M_1 := (S \otimes k V_1)^G = \{ f \in S \mid \sigma \cdot f = (\text{sgn } \sigma) f \} = (x-y)R \cong R.$$ 

So $eR$ also decompose as $eR \cong M_1^{\sigma}$. Therefore, the uniqueness doesn’t hold in this case.

### 3. Generalized $F$-signature of invariant subrings

In this section, we show the existence of the limit and determine it.

In our case, the invariant subring $R$ has FFRT. Thus, the existence of the limit $\lim_{e \to \infty} \frac{c_{i,e}}{pde}$ is guaranteed by the next proposition. So we can define this limit.

**Proposition 3.1** ([SVdB], [Yao1]). If $R$ has FFRT, then for $i = 0, 1, \cdots, n$, the limit $\lim_{e \to \infty} \frac{c_{i,e}}{pde}$ exists.

**Remark 3.2.** In [SVdB], this proposition is proved under the assumption “$R$ is strongly $F$-regular and has FFRT”. After that, Y. Yao showed the condition of strongly $F$-regular is unnecessary [Yao1]. Note that the existence of the limit for free direct summands (i.e. $F$-signature) is proved under more general settings as we showed before.

**Definition 3.3.** We call this limit the generalized $F$-signature of $M_i$ and denote it by

$$s(R, M_i) := \lim_{e \to \infty} \frac{c_{i,e}}{pde}.$$ 

The main theorem in this paper is the following.

**Theorem 3.4** (Main theorem). Let the notation be as above. Then for all $i = 0, \cdots, n$ one has

$$s(R, M_i) = \frac{\dim_k V_i}{|G|} = \frac{\text{rank}_R M_i}{|G|}.$$ 

**Remark 3.5.** The second equation follows from $\dim_k V_i = \text{rank}_R M_i$ clearly.

The case that $i = 0$ is due to [WY], as we have seen before (Theorem 1.4). And a similar result holds for finite subgroup scheme of $\text{SL}_2$ [HS].

**Remark 3.6.** From this theorem, we can see that each indecomposable MCM $R$-modules in the finite set $\{ R, M_1, \cdots, M_{n-1} \}$ actually appear in $eR$ as a direct summand for sufficiently large $e$ (see also [TY, Proposition 2.5]).
In order to prove this theorem, we introduce the notion of the Brauer character. In the representation theory of finite groups over \( \mathbb{C} \), the character gives us very effective method to distinguish each representation. But now, we are in a positive characteristic field \( k \), not in \( \mathbb{C} \). So the character in the original sense doesn’t work well. Therefore we have to modify it for applying to our context. For this purpose, we introduce the Brauer character (for more details, refer to some textbooks e.g. [CR], [Wei]).

Firstly, we take an element \( g \in G \) and suppose that the order of \( g \) is \( m \). Then each eigenvalues of \( g \) is a primitive \( m \)-th root of unity. Let \( \omega_1, \cdots, \omega_d \) be eigenvalues of \( g \). Since \( (m, p) = 1 \), \( \omega_1, \cdots, \omega_d \) are in \( k \). And such elements form a cyclic group of order \( m \);

\[
\mu_m(k) := \{ \omega \in k^\times \mid \omega^m = 1 \} \subset k^\times.
\]

Furthermore, there exists an isomorphism

\[
\Phi : \mu_m(k) \xrightarrow{\cong} \mu_m(\mathbb{C}) := \{ \omega \in \mathbb{C}^\times \mid \omega^m = 1 \}.
\] (3.1)

By using this notation, we can define the Brauer character as follows.

**Definition 3.7.** For a \( kG \)-module \( V \), the Brauer character \( \chi_V \) of \( V \) is the function \( \chi_V : G \to \mathbb{C} \) given by

\[
\chi_V(g) := \sum_{i=1}^{d} \Phi(\omega_i) \in \mathbb{C} \quad (g \in G),
\]

where \( \omega_1, \cdots, \omega_d \) are the eigenvalues of \( g \).

Since the value of the Brauer character is in \( \mathbb{C} \), we can discuss the limit of this character. The following proposition is well-known for the original character over \( \mathbb{C} \). And this kind of formula also holds for the Brauer character. The proof is almost the same as the original one through an isomorphism (3.1).

**Proposition 3.8.** Let \( V, W \) be \( kG \)-modules and \( g \in G \), then

1. \( \chi_{V \otimes W}(g) = \chi_V(g) \cdot \chi_W(g) \).
2. \( \chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g) \).
3. \( \chi_{V^*}(g) = \chi_V(g) \).
4. \( \dim_k \text{Hom}_G(V, W) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \cdot \chi_W(g) \).
5. \( \chi_V(1_G) = \dim_k V \).

So we are now ready to prove the main theorem.

**Proof of Theorem 3.4.** Firstly, there is \( e_0 \geq 1 \) such that the group ring \( \mathbb{F}_{q_0} G \) is isomorphic to the direct product of total matrix rings over \( \mathbb{F}_{q_0} \), where \( q_0 = p^{e_0} \). Namely,

\[
\mathbb{F}_{q_0} G \cong \text{Mat}_{r_1}(\mathbb{F}_{q_0}) \times \cdots \times \text{Mat}_{r_m}(\mathbb{F}_{q_0}), \quad (r_1, \cdots, r_m \in \mathbb{N}).
\]

Since the component of matrix representation of Frobenius twist is \( p^{-e_0} \)-th power of the original one, so if we take an appropriate basis, then any component of matrix representation is in the finite field \( \mathbb{F}_{q_0} \). Thus, if \( e = e_0 t \), then we can consider \( ^t M \cong M \) for any \( G \)-module \( M \).
Since we know the existence of the limit, it suffices to show the subsequence \( \{ c_{i,e} \}_{e \in \mathbb{N}} \) converge on \((\dim_k V_i)/|G|\). So we prove
\[
\lim_{e \to \infty} \frac{c_{i,e}}{q^{de_{i,e}}} = \frac{\dim_k V_i}{|G|}.
\]

For \( e = e_0 \), we obtain \( \epsilon S/m^\epsilon S \cong \epsilon(S/m[q]) \cong S/m[q] \). And \( S/m^\epsilon S \) is also isomorphic to the finite direct sum of irreducible representations (cf. Proposition 2.2). By Proposition 3.8 (4), the multiplicity \( c_{i,e} \) is described as follows.
\[
c_{i,e} = \dim_k \text{Hom}_G(V_i,S/m[q]) = \frac{1}{|G|} \sum_{g \in G} \chi_{V_i}(g) \cdot \chi_{S/m[q]}(g).
\]

Set \( g \in G \) and suppose that the order \( g \) is \( m \). Then there is a basis \( \{x_1, \cdots, x_d\} \) of \( V \) such that each \( x_i \) is an eigenvector of \( g \) and we can write \( g \cdot x_i = \omega x_i \) with \( \omega = \omega^\delta \) for some \( 0 \leq \delta < m \), where \( \omega \) is a primitive \( m \)-th root of unity. In this situation
\[
\{x_1^{\lambda_1} \cdots x_d^{\lambda_d} \mid 0 \leq \lambda_1, \ldots, \lambda_d < q\} \subset \bigoplus_{l=0}^{(q-1)d} \text{Sym}_l V
\]
is a basis of \( S/m[q] \). As each \( x_1^{\lambda_1} \cdots x_d^{\lambda_d} \) is an eigenvector of \( g \) with the eigenvalue \( \omega^{\lambda_1} \cdots \omega^{\lambda_d} \), we have
\[
\chi_{S/m[q]}(g) = \sum_{0 \leq \lambda_1, \ldots, \lambda_d < q} \Phi(\omega^{\lambda_1} \cdots \omega^{\lambda_d}) = \prod_{i=1}^d (1 + \theta_i + \cdots + \theta_i^{q-1}),
\]
where \( \theta_i := \Phi(\omega_i) \).

(i) In case \( g = 1 \), by Proposition 3.8 (5),
\[
\frac{\chi_{V_i}(g) \cdot \chi_{S/m[q]}(g)}{q^{d}} = \frac{\dim_k V_i \cdot q^{d}}{q^d} = \dim_k V_i.
\]

(ii) In case \( g \neq 1 \), we may assume \( \theta_d \neq 1 \). Then
\[
\left| \frac{\chi_{V_i}(g) \cdot \chi_{S/m[q]}(g)}{q^{d}} \right| \leq \left| \frac{\chi_{V_i}(g)}{q^{d}} \right| \prod_{i=1}^{d-1} (|1| + |\theta_i| + \cdots + |\theta_i|^{q-1}) \cdot \left| \frac{1 - \theta_d^q}{1 - \theta_d} \right|
\]
\[
\leq \frac{\dim_k V_i}{q} \cdot \frac{2}{|1 - \theta_d|} \to 0 \quad \text{as} \quad e \to \infty.
\]
The first inequation is obtained by applying the triangle inequality. Since \( |\theta_i| \leq 1 \), we can obtain the second inequation.

From previous arguments, we may only discuss in case \( g = 1 \). Thus, we conclude
\[
\lim_{e \to \infty} \frac{c_{i,e}}{q^{d}} = \lim_{e \to \infty} \frac{1}{q^{d}} \cdot \frac{1}{|G|} \sum_{g \in G} \chi_{V_i}(g) \cdot \chi_{S/m[q]}(g) = \frac{\dim_k V_i}{|G|}.
\]
Combining this theorem and [SVdB, Proposition 3.3.1, Lemma 3.3.2], we immediately have the next corollary.

**Corollary 3.9.** If $e M_i$ decompose as follows

$$e M_i \cong M_0^{d_0^{d_{i,e}}} \oplus M_1^{d_1^{d_{i,e}}} \oplus \cdots \oplus M_n^{d_n^{d_{i,e}}} ,$$

then for all $i, j = 0, \cdots, n$ one has

$$s(M_i, M_j) := \lim_{\epsilon \to \infty} \frac{d_i^{d_{i,e}}}{p^{d_{i,e}}} = \frac{(\dim_k V_i) \cdot s(R, M_j)}{|G|} = \frac{(\dim_k V_i) \cdot (\dim_k V_j)}{|G|} = \frac{(\text{rank}_R M_i) \cdot (\text{rank}_R M_j)}{|G|}.$$