S. Brochard *et al.* (2022) “Wiles Defect for Modules and Criteria for Freeness,”
International Mathematics Research Notices, Vol. 00, No. 0, pp. 1–23
https://doi.org/10.1093/imrn/rnac052

Wiles Defect for Modules and Criteria for Freeness

Sylvain Brochard[1], Srikanth B. Iyengar[2,*], and Chandrashekhar B. Khare[3]

[1]IMAG, University of Montpellier, CNRS, Montpellier, France, [2]Department of Mathematics, University of Utah, Salt Lake City, UT 84112, USA, and [3]Department of Mathematics, University of California, Los Angeles, CA 90095, USA.

[*]*Correspondence to be sent to: e-mail: iyengar@math.utah.edu*

Diamond proved a numerical criterion for modules over local rings to be free modules over complete intersection rings. We formulate a refinement of these results using the notion of *Wiles defect*. A key step in the proof is a formula that expresses the Wiles defect of a module in terms of the Wiles defect of the underlying ring.

1 Introduction

In his work on modularity of elliptic curves and Fermat’s last theorem, Wiles [17] discovered a numerical criterion for certain noetherian local rings A to be complete intersections. Diamond [8] generalized Wiles’ result by establishing a criterion for modules M over A to be free and for A to be a complete intersection; see the discussion below for the precise statements of their results.

To set the stage for our work, we recall the number theoretic application of the numerical criterion, although this paper concerns only its commutative algebraic aspects. The ring of interest is a deformation ring R associated to a modular representation $\overline{\rho}\colon G_{\mathbb{Q}} \to GL_2(k)$, with $G_{\mathbb{Q}}$ the absolute Galois group of $\mathbb{Q}$. Here $\overline{\rho}$ arises from a Hecke algebra $\mathbb{T}$ (which is a complete, Noetherian, local $\mathcal{O}$-algebra) acting faithfully on $H^1(X_0(N), \mathcal{O})_{\mathfrak{m}}$, the cohomology of a modular curve $X_0(N)$, associated to

Received July 18, 2021; Revised February 8, 2022; Accepted February 18, 2022

a positive integer N, with coefficients in a discrete valuation ring $\mathcal{O}$ finite flat over $\mathbb{Z}_p$, localized at the maximal ideal $\mathfrak{m}$, and with $\mathbb{T}/\mathfrak{m} = k$ a finite field. There is an action of $G_{\mathbb{Q}}$ on $H^1(X_0(N), \mathcal{O})_{\mathfrak{m}}$ and the representation $\overline{\rho}$ is isomorphic to the representation $\overline{\rho}_{\mathfrak{m}} : G_{\mathbb{Q}} \to GL_2(\mathbb{T}/\mathfrak{m})$ associated to $\mathfrak{m}$. This produces a surjective map $R \to \mathbb{T}$, and the numerical criterion implies in favorable conditions that $H^1(X_0(N), \mathcal{O})_{\mathfrak{m}}$ is free as an R-module and that R is a complete intersection. In particular, the map $R \to \mathbb{T}$ is an isomorphism of complete intersections. In practice, this is used to deduce that a certain ring R' (parametrizing deformations of $\overline{\rho}$ with ramification allowed at a prime q) acts freely on $H^1(X_0(Nq^2), \mathcal{O})_{\mathfrak{m}'}$, where $\mathfrak{m}'$ is a maximal ideal of the Hecke algebra acting on $H^1(X_0(Nq^2), \mathcal{O})$, related to $\mathfrak{m}$, from knowing that a quotient R of R' acts freely on $H^1(X_0(N), \mathcal{O})_{\mathfrak{m}}$.

The main contribution of the present work is a criterion for freeness of a module in terms of its *Wiles defect*, which was introduced in [3]; the definition is recalled below. This refines the work of Diamond and Wiles and also gives a new perspective on these earlier results from the vantage point of the Wiles defect of rings and of modules over them. Our proofs differ significantly from those in loc. cit.

The setting for all the results of Wiles and Diamond, and the present paper, is that there is a commutative, noetherian, local ring A equipped with a surjective map $\lambda \colon A \to \mathcal{O}$, where $\mathcal{O}$ is a discrete valuation ring (that will be fixed throughout the paper), with the property that the conormal module

$$\Phi_A := \mathfrak{p}_A/\mathfrak{p}_A^2 \quad \text{where } \mathfrak{p}_A := \operatorname{Ker}(\lambda),$$

has finite length as an $\mathcal{O}$-module. (In the work of Diamond and Wiles, A would be a finite $\mathcal{O}$-algebra and λ a map of $\mathcal{O}$-algebras, but we do not impose this.) The *congruence module* of a finitely generated A-module M is the A-module

$$\Psi_A(M) := \frac{M}{M[\mathfrak{p}_A] + M[I_A]}, \quad \text{where } I_A := A[\mathfrak{p}_A].$$

Here, for any ideal $\mathfrak{a}$ in A we write $M[\mathfrak{a}]$ for $\{m \in M \mid \mathfrak{a} \cdot m = 0\}$, the $\mathfrak{a}$-torsion submodule of M. As $\mathfrak{p}_A \cdot \Psi_A(M) = 0$, the congruence module $\Psi_A(M)$ has a natural structure of an $\mathcal{O}$-module. Moreover, the hypothesis that Φ_A has finite length implies that the same is true of $\Psi_A(M)$. Also $M[\mathfrak{p}_A]$ has a natural structure of an $\mathcal{O}$-module, and we can consider its rank. Observe that the rank of $M[\mathfrak{p}_A]$ equals the dimension of $M_{\mathfrak{p}_A}$ over the fraction field of $\mathcal{O}$, and in particular they are nonzero precisely when M is supported at $\mathfrak{p}_A$. This is the main case of interest in this work.

The *Wiles defect* of the A-module M is the integer

$$\delta_A(M) = d \cdot \operatorname{length}_{\mathcal{O}} \Phi_A - \operatorname{length}_{\mathcal{O}} \Psi_A(M), \tag{1.1}$$

where $d := \operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]$. In [2, 3], this number is divided by de, where e is the ramification index of $\mathcal{O}$. We find it more convenient to suppress the denominator.

We prove

Theorem 1.1. Let M be a finitely generated A-module with $\operatorname{depth}_A M \geq 1$. There is an equality

$$\operatorname{length}_{\mathcal{O}} \Psi_A(M) = (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]) \cdot \operatorname{length}_{\mathcal{O}} \Psi_A(A) - \operatorname{length}_{\mathcal{O}} (M[\mathfrak{p}_A]/I_A M) .$$

Equivalently, there is an equality

$$\delta_A(M) = (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]) \cdot \delta_A(A) + \operatorname{length}_{\mathcal{O}} (M[\mathfrak{p}_A]/I_A M) .$$

In particular $\delta_A(M) \geq 0$. If $M_{\mathfrak{p}_A} \neq 0$ and $\delta_A(M) = 0$, then A is complete intersection and M is faithful. When in addition, M has rank at most $\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]$ at each generic point of A, then M is free.

The 1st part of this result, relating the lengths of the congruence modules of M and of A, is contained in Theorem 3.3. The last part of Theorem 1.1, describing when $\delta_A(M) = 0$ is suggested by, and refines, the result of Diamond [8, Theorem 2.4]; see Theorem 4.6 and also the result below. In [8] the module M is required to be finite flat over $\mathcal{O}$; we replace this by the weaker condition that M is finitely generated over A and of positive depth.

One input in its proof is a result of [9] that dealt with the case M is a cyclic A-module; see Theorem 4.5 below. The main new ingredient is the following criterion for freeness of modules.

Theorem 1.2. Suppose that the ring A is Gorenstein and that M is a finitely generated A-module with $\operatorname{depth}_A M \geq 1$. If

$$\delta_A(M) = (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A])\delta_A(A) ,$$

and M has rank at most $\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]$ at each generic point of A, then M is free.

This result is implied by Theorem 4.3, where the condition on ranks is replaced by a weaker one involving multiplicities.

The proofs of Theorems 1.1 and 1.2 are based on a careful study of congruence modules, and various other auxiliary modules related to them. This is the contents of Sections 2 and 3. In Section 5, we give a more streamlined proof of a formula for $\delta_A(A)$, formulated (albeit in the setting of certain derived rings) by Venkatesh [16], and proved in [10], in terms of certain André–Quillen cohomology modules. We end by explaining how this formula gives another proof of the isomorphism criterion for maps between complete intersection rings due to Wiles [17] and Lenstra [13].

We end the introduction by expanding on the potential significance of Theorem 1.1 for the study of congruences between modular forms. The question of comparing congruence modules for A and M has been studied extensively, in the context of the theory of congruences between modular forms. This theory plays a key role in the breakthrough work of Wiles [17]. As recalled above, one studies a Hecke algebra $\mathbb{T}$ acting on $H^1(X_0(N), \mathcal{O})_{\mathfrak{m}}$ that is isomorphic to $M \oplus M$ where M is $\mathbb{T}$-module that is finite flat over $\mathcal{O}$, and hence of positive depth, and of generic rank one as a $\mathbb{T}$-module. One focuses on an augmentation $\lambda_f = \lambda \colon \mathbb{T} \to \mathcal{O}$ arising from a weight 2 newform $f \in S_2(\Gamma_0(N))$. In this context, the question of showing that the congruence modules for $\mathbb{T}$ and M (associated to the augmentation λ_f arising from the newform f) are the same has been studied in works of Hida [11] and Ribet [14] in 1980s and in many other works, including [17]. The motivation for doing this is that the (cohomological) congruence module of M is easier to study and related to a critical value of the L-function associated to the adjoint motive of f (as discovered by Hida in his seminal work), while the congruence module for $\mathbb{T}$ is more directly related to congruences between f and other newforms in $S_2(\Gamma_0(N))$. In these works, it was shown that the natural surjection $\Psi_{\mathbb{T}}(\mathbb{T}) \to \Psi_{\mathbb{T}}(M)$ is an isomorphism, thus proving that all congruences between f and other newforms in $S_2(\Gamma_0(N))$ are detected "cohomologically", by showing that M is a free $\mathbb{T}$-module (of rank 1). It follows from our results that such an isomorphism holds precisely when $M[\mathfrak{p}_A]/I_A M = 0$, which can happen without M being free over $\mathbb{T}$. For instance, [2, Theorem 3.12] implies that $M[\mathfrak{p}_A]/I_A M = 0$ when $\mathrm{End}_{\mathbb{T}}(M) = \mathbb{T}$, which is a weaker condition than freeness. We hope the observation recorded in the 1st part of Theorem 1.1, which gives meaning to the kernel of the surjective map $\Psi_{\mathbb{T}}(\mathbb{T}) \to \Psi_{\mathbb{T}}(M)$, will be useful in the further study of congruences between modular forms.

2 The Category $\mathsf{C}_{\mathcal{O}}$

Throughout this work, $\mathcal{O}$ is a discrete valuation ring and ϖ a uniformizing parameter for $\mathcal{O}$. We write $\mathsf{C}_{\mathcal{O}}$ for the category consisting of pairs (A, λ_A) where A is a commutative, noetherian, local ring and $\lambda_A \colon A \to \mathcal{O}$ is a surjective map of rings such that the conormal module $\Phi_A := \mathfrak{p}_A/(\mathfrak{p}_A)^2$, where $\mathfrak{p}_A := \mathrm{Ker}(\lambda_A)$, has finite length. The morphisms in $\mathsf{C}_{\mathcal{O}}$ are local maps $\varphi \colon A \to B$ such that $\lambda_B \varphi = \lambda_A$. The rings in $\mathsf{C}_{\mathcal{O}}$ have the same residue field, namely, $\mathcal{O}/\varpi\mathcal{O}$.

The condition that the conormal module of A has finite length is equivalent to the natural map $A_{\mathfrak{p}_A} \to \mathcal{O}_{(0)}$ being an isomorphism; here $\mathcal{O}_{(0)}$ is the quotient field of $\mathcal{O}$. Thus, $\mathfrak{p}_A$ is a minimal prime of A and $\dim A/\mathfrak{p}_A = \dim \mathcal{O} = 1$. This has the following consequence. Subject to the constraint that $\operatorname{depth} A \le 1$, the pair $(\operatorname{depth} A, \dim A)$ can take all possible values; see Example 2.

Lemma 2.1. For any $A \in \mathsf{C}_{\mathcal{O}}$, one has $\operatorname{depth} A \le 1 \le \dim A$.

Proof. The claim about dimension is clear from the surjection $A \to \mathcal{O}$. Any associated prime $\mathfrak{q}$ of A satisfies $\operatorname{depth} A \le \dim A/\mathfrak{q}$; see [5, Proposition 1.2.13]. Setting $\mathfrak{q} := \mathfrak{p}_A$ yields the upper bound on the depth of A. ■

Let A be in $\mathsf{C}_{\mathcal{O}}$ and set $I_A := A[\mathfrak{p}_A]$, the annihilator of $\mathfrak{p}_A$. In addition, the following objects also play an important role in this work:

$$\Psi_A := \mathcal{O}/\lambda(I_A) \quad \text{and} \quad \frac{I_A}{I_A^2}\,.$$

The 1st one is the *congruence algebra* of A, and the last one is the conormal module of the map $A \to A/I_A$. Since $\mathfrak{p}_A \cdot I_A = 0$ the A-action on I_A factors through $\mathcal{O}$, and so the A-action on I_A/I_A^2 factors through Ψ_A. By the same token, Φ_A is a Ψ_A-module.

Set $K := \mathcal{O}_{(0)}$, the field of fractions of $\mathcal{O}$. Viewing I_A as an $\mathcal{O}$-module, one has

$$(I_A)_{(0)} \cong \mathrm{Hom}_A(\mathcal{O}, A)_{\mathfrak{p}_A} \cong \mathrm{Hom}_{A_{\mathfrak{p}_A}}(K, A_{\mathfrak{p}_A}) \cong \mathrm{Hom}_K(K,K) \cong K\,. \tag{2.1}$$

Thus, $\operatorname{rank}_{\mathcal{O}}(I_A) = 1$. It also follows that $I_A \not\subseteq \mathfrak{p}_A$, for $\mathfrak{p}_A A_{\mathfrak{p}_A} = 0$, so $\lambda(I_A) \ne 0$; equivalently, that Ψ_A is a torsion $\mathcal{O}$-module, that is to say, of finite length. In fact, since the Fitting ideal of $\mathfrak{p}_A$ is contained in its annihilator, one gets an inequality

$$\operatorname{length}_{\mathcal{O}} \Phi_A \ge \operatorname{length}_{\mathcal{O}} \Psi_A\,. \tag{2.2}$$

See [7, Section 5, (5.2.3)]. Wiles and Lenstra proved that equality holds if and only if the ring A is complete intersection; see Theorem 4.5.

Evidently, $\mathfrak{p}_A \subseteq A[I_A]$ but in fact equality always holds.

Lemma 2.2. For any A in $\mathsf{C}_{\mathcal{O}}$ one has $\mathfrak{p}_A = A[I_A]$.

Proof. One has $\lambda(A[I_A]) \cdot \lambda(I_A) = \lambda(A[I_A] \cdot I_A) = 0$. Since $\mathcal{O}$ is a domain and $\lambda(I_A)$ is nonzero, it follows that $\lambda(A[I_A]) = 0$, that is to say, $A[I_A] \subseteq \mathfrak{p}_A$. ■

The following computation will be useful later on. The hypothesis on depth is needed even for the weaker conclusion; see 2.

Lemma 2.3. Let A be an object in $\mathsf{C}_{\mathcal{O}}$ and M a finitely generated A-module. When $\operatorname{depth}_A M \geq 1$, one has $M[\mathfrak{p}_A] \cap M[I_A] = (0)$; in particular, $I_A M \cap \mathfrak{p}_A M = 0$.

Proof. The A-modules $M[\mathfrak{p}_A]$ and $M[I_A]$ are annihilated by $\mathfrak{p}_A$ and I_A, respectively. Thus, $M[\mathfrak{p}_A] \cap M[I_A]$ is annihilated by $\mathfrak{p}_A + I_A$. This ideal contains some power of the maximal ideal of A, and hence it contains an element that is not a zero divisor on M, since the latter has positive depth. Thus, $M[\mathfrak{p}_A] \cap M[I_A] = (0)$. ■

The conormal module and congruence module are related: since A-acts on I_A through $\mathcal{O}$, one gets isomorphisms

$$\frac{I_A}{I_A^2} \cong I_A \otimes_A \frac{A}{I_A} \cong I_A \otimes_{\mathcal{O}} (\mathcal{O} \otimes_A \frac{A}{I_A}) \cong I_A \otimes_{\mathcal{O}} \Psi_A \,. \tag{2.3}$$

Here is another expression of the relation between all these invariants

$$\frac{I_A}{I_A^2} \otimes_{(A/I_A)} \mathfrak{p}_A \cong I_A \otimes_A \mathfrak{p}_A \cong I_A \otimes_{\mathcal{O}} \frac{\mathfrak{p}_A}{\mathfrak{p}_A^2} \,.$$

To put this isomorphism in a larger context, it helps to remark that

$$\mathfrak{p}_A = \operatorname{Hom}_A(A/I_A, A) \quad \text{and} \quad I_A = \operatorname{Hom}_A(\mathcal{O}, A)\,,$$

where the 1st equality is by Lemma 2.2 and the 2nd is by definition. These are the relative dualizing modules for the maps $A \to A/I_A$ and $A \to \mathcal{O}$, respectively. Here is one consequence of these observations.

Lemma 2.4. Let A be an object in $\mathsf{C}_{\mathcal{O}}$. When $\operatorname{depth} A = 1$, the ideal $I_A \subset A$ is principal and as a Ψ_A-module I_A/I_A^2 is free of rank one.

Proof. By Lemma 2.3, the hypothesis that $\operatorname{depth} A \geq 1$ implies $I_A \cap \mathfrak{p}_A = 0$, so the composition $I_A \to A \to \mathcal{O}$ is injective. Thus, as an $\mathcal{O}$-module I_A is free and of rank one; in particular $I_A \subset A$ is principal. Moreover, (2.3) implies that as a Ψ_A-module I_A/I_A^2 is free of rank one. ■

After suitable completion, any A in $\mathsf{C}_{\mathcal{O}}$ is of the form $\mathcal{O}[\![\boldsymbol{x}]\!]/J$, for indeterminates $\boldsymbol{x} := x_1, \ldots, x_n$, and $J \subseteq \varpi(\boldsymbol{x}) + (\boldsymbol{x})^2$. One has $\mathfrak{p}_A := (\boldsymbol{x})$. Let $f_1, \ldots, f_c$ be a minimal generating set for the ideal J. For each i, there is an unique expression of the form

$$f_i = \sum a_{ij} x_j + \text{term in } (\boldsymbol{x})^2 \,,$$

with a_{ij} in $\mathcal{O}$. It is easy to verify that the conormal module of λ_A has a presentation

$$\mathcal{O}^c \xrightarrow{(a_{ij})} \mathcal{O}^n \longrightarrow \Phi_A \longrightarrow 0\,.$$

Thus, the condition that Φ_A has finite length is equivalent to $\operatorname{rank}(a_{ij}) = n$; equivalently, $\operatorname{Fitt}_0(a_{ij})$, the zeroth Fitting ideal of the $\mathcal{O}$-module Φ_A, is nonzero. Using this, or even directly, one can verify that the ring

$$A := \frac{\mathcal{O}[\![x_1, \ldots, x_n]\!]}{(\varpi x_1, \ldots, \varpi x_n)}$$

is in $\mathsf{C}_{\mathcal{O}}$. The associated primes of A are (ϖ) and $(\boldsymbol{x})$, so it follows that $\dim A = n$ and $\operatorname{depth} A = 1$. This shows that for each positive integer n, one has rings A in $\mathsf{C}_{\mathcal{O}}$ with $\operatorname{depth} A = 1$ and $\dim A = n$; see Lemma 2.1. In the same vein, the ring $A/x_1(\boldsymbol{x})$ satisfies $\dim A = n - 1$ and $\operatorname{depth} A = 0$.

The next example shows that the condition $\operatorname{depth} A \geq 1$ in Lemma 2.3 is not superfluous.

When $A := \mathcal{O}[\![x]\!]/(\varpi x, x^2)$, one has

$$\mathfrak{p}_A = (x) \subseteq I_A = (\varpi, x)\,.$$

Thus, $I_A \cap \mathfrak{p}_A = \mathfrak{p}_A$.

Next we describe a ring in the category $\mathsf{C}_{\mathcal{O}}$ that is Gorenstein, but not complete intersection. This is in anticipation of Theorem 4.3.

Assume 2 is invertible in $\mathcal{O}$ and consider the ring

$$A := \frac{\mathcal{O}[\![x,y,z]\!]}{(x^2-y^2, x^2-z^2, \varpi x - yz, \varpi y - xz, \varpi z - xy)} .$$

From 2, one gets that $\Phi_A \cong k^3$, where $k := \mathcal{O}/(\varpi)$. In particular, A is in $\mathsf{C}_{\mathcal{O}}$. We claim that the ring A is reduced, Gorenstein of Krull dimension one, but not complete intersection. It is also finite and free as an $\mathcal{O}$-module.

Indeed, as an $\mathcal{O}$-module, A has a basis consisting of (residue classes of) elements $1, x, y, z, x^2$, so that A is finite and free over $\mathcal{O}$. In particular, ϖ is not a zero-divisor on A. The ring $A/(\varpi)$ is zero-dimensional, with socle the ideal (x^2), and hence it is Gorenstein; however, it is not a complete intersection, for it has embedding dimension three, but five defining relations; see [5, Example 3.2.11(b)]. Thus, A itself is Gorenstein of Krull dimension one and not complete intersection.

It remains to verify that A is reduced. A straightforward calculation yields that the prime ideals in A are

$$(\varpi, x, y, z)\,, \quad (x, y, z)\,, \quad (x-\varpi, y-\varpi, z-\varpi)$$
$$(x+\varpi, y+\varpi, z-\varpi)\,, \quad (x+\varpi, y-\varpi, z+\varpi)\,, \quad (x-\varpi, y+\varpi, z+\varpi)\,.$$

In this list, the 1st one is the maximal ideal; the rest are minimal. The localization of A at any minimal prime is a field. Since A is Cohen–Macaulay of dimension one, it thus satisfies Serre conditions (S_1) and (R_0) and hence is reduced.

3 Congruence Modules

In this section, we develop basic properties of congruence modules for modules over rings in $\mathsf{C}_{\mathcal{O}}$. This prepares us for the next section where we obtain criteria for freeness of the modules in terms of Wiles defects of the modules in question. We begin by recording an observation that will be used multiple times in the sequel.

Lemma 3.1. Let J be an ideal in a ring A and M an A-module. If $x \in A$ is not a zerodivisor on M, then

$$xM \cap M[J] = x(M[J])\,.$$

Thus, when A is local, M is finitely generated, and x in not a unit in A, either $M[J] = 0$ or $M[J] \not\subseteq xM$.

Proof. Indeed, for any m in M if $(xm)\cdot J = 0$, then $m \cdot J = 0$ for x is not a zero divisor on M, and hence m is in $M[J]$, as desired. The 2nd part of the claim is by Nakayama's Lemma, applied to $M[J]$. ■

3.1 Congruence modules

Let A be an object in $\mathsf{C}_{\mathcal{O}}$ and M a finitely generated A-module. As in the Introduction, the *congruence module* of M is

$$\Psi_A(M) := \frac{M}{M[\mathfrak{p}_A] + M[I_A]}\,.$$

We write Ψ_A, instead of $\Psi_A(A)$; observe that this agrees with the definition introduced in 2, for $A[I_A] = \mathfrak{p}_A$, by Lemma 2.2. Evidently, $\Psi_A(M)$ is a finitely generated module over the congruence algebra Ψ_A. Next we describe a canonical presentation of the congruence module.

Observe that the A-modules $M[\mathfrak{p}_A]$ and $M/M[I_A]$ are annihilated by $\mathfrak{p}_A$ and hence are naturally $\mathcal{O}$-modules.

Lemma 3.2. When $\operatorname{depth}_A M \geq 1$, the $\mathcal{O}$-modules $M[\mathfrak{p}_A]$ and $M/M[I_A]$ are free of the same rank, and the following natural sequence of $\mathcal{O}$-modules is exact:

$$0 \longrightarrow M[\mathfrak{p}_A] \longrightarrow \frac{M}{M[I_A]} \longrightarrow \Psi_A(M) \longrightarrow 0\,.$$

Proof. The exactness of the sequence is immediate from the definition of Ψ_A and Lemma 2.3. The main task is to verify the claims about freeness. Since $M[\mathfrak{p}_A]$ is an A-submodule of M and the latter has positive depth, so does the former. The A-action on $M[\mathfrak{p}_A]$ factors through $\mathcal{O}$ so $\operatorname{depth}_{\mathcal{O}} M[\mathfrak{p}_A] \geq 1$ and so $M[\mathfrak{p}_A]$ is free.

Since $\operatorname{depth}_A M \geq 1$, there exists a non-unit element $x \in A$ that is not a zero divisor on M. We claim that x is not a zero divisor on $M/M[I_A]$ as well.

Indeed, suppose x annihilates the residue class in $M/M[I_A]$ of an element $m \in M$, that is to say, $xm \in M[I_A]$. Then

$$xm \in xM \cap M[I_A] = x(M[I_A])\,,$$

where the equality is by Lemma 3.1. Thus, $xm = xm'$ for some $m' \in M[I_A]$, and hence $m = m'$, as x is not a zero divisor on M. Thus, m is zero in $M/M[I_A]$.

Since $M/M[I_A]$ has positive depth, it too is free as an $\mathcal{O}$-module. ■

We also consider the following variant of the congruence module:

$$\hat{\Psi}_A(M) := \frac{M}{M[I_A] + I_A M}\,.$$

Lemma 2.2 implies that $\hat{\Psi}_A(A) = \Psi_A$, so that $\hat{\Psi}_A(M)$ is a Ψ_A-module, namely a quotient of the Ψ_A-module $\Psi_A \otimes_A M$, and they are equal when M is free as an A-module. It is easy to verify that there is an exact sequence of Ψ_A-modules:

$$0 \longrightarrow \frac{M[\mathfrak{p}_A]}{I_A M + (M[\mathfrak{p}_A] \cap M[I_A])} \longrightarrow \hat{\Psi}_A(M) \longrightarrow \Psi_A(M) \longrightarrow 0\,. \tag{3.1}$$

Keep in mind that $M[\mathfrak{p}_A] \cap M[I_A] = 0$ when $\operatorname{depth}_A M \geq 1$, by Lemma 2.3.

These observations serve to establish the connection between the Wiles defect (1.1) of A and of M. This settles the 1st part of Theorem 1.1. As in *op. cit.* one could state the equality in terms of congruence modules of A and M.

Theorem 3.3. Let A be an object in $\mathsf{C}_{\mathcal{O}}$ and M a finitely generated A-module. When $\operatorname{depth}_A M \geq 1$, there is an equality

$$\delta_A(M) = (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]) \cdot \delta_A(A) + \operatorname{length}_{\mathcal{O}} (M[\mathfrak{p}_A]/I_A M)\,.$$

In particular, $\delta_A(M) \geq 0$.

Proof. Observe that for any A-module M there is an isomorphism of Ψ_A-modules

$$\hat{\Psi}_A(M) \cong \Psi_A \otimes_{\mathcal{O}} \frac{M}{M[I_A]}\,.$$

Since $\operatorname{depth}_A M \geq 1$, the $\mathcal{O}$-modules $M/M[I_A]$ and $M[\mathfrak{p}_A]$ are free of the same rank, by Lemma 3.2, so the isomorphism above yields the equality

$$\operatorname{length}_{\mathcal{O}} \hat{\Psi}_A(M) = (\operatorname{length}_{\mathcal{O}} \Psi_A) d,$$

where $d := \operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]$. This justifies the 3rd equality below.

$$\begin{aligned}\delta_A(M) &= d \cdot \operatorname{length}_{\mathcal{O}} \Phi_A - \operatorname{length}_{\mathcal{O}} \Psi_A(M)\\ &= d \cdot \operatorname{length}_{\mathcal{O}} \Phi_A - \operatorname{length}_{\mathcal{O}} \hat{\Psi}_A(M) + \operatorname{length}_{\mathcal{O}} (M[\mathfrak{p}_A]/I_A M)\\ &= d \cdot \operatorname{length}_{\mathcal{O}} \Phi_A - d \cdot \operatorname{length}_{\mathcal{O}} \Psi_A + \operatorname{length}_{\mathcal{O}} (M[\mathfrak{p}_A]/I_A M)\\ &= d \cdot \delta_A(A) + \operatorname{length}_{\mathcal{O}} (M[\mathfrak{p}_A]/I_A M)\,.\end{aligned}$$

The 1st and the last equalities are the definition of defects (1.1) while the 2nd one is from (3.1) and Lemma 2.3. The last equality also uses the observation that the rank of the $\mathcal{O}$-module $A[\mathfrak{p}_A] = I_A$ is one; see (2.1).

The last conclusion holds because $\delta_A(A) \geq 0$; see (2.2). ■

It follows from the proof above that when $\operatorname{depth}_A M \geq 1$ and $\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A] = 1$, there is a surjective map $\Psi_A \twoheadrightarrow \Psi_A(M)$, with kernel $M[\mathfrak{p}_A]/I_A M$.

In the next lemma, we show that the congruence module for modules M of positive depth remains invariant under pull-back of rings. We use this in the proof of Theorem 4.6.

Lemma 3.4. Let $A \to B$ be a surjective map in $\mathsf{C}_{\mathcal{O}}$ and M a finitely generated B-module. One has a natural surjection

$$\Psi_B(M) \twoheadrightarrow \Psi_A(M)\,.$$

This map is bijective when $\operatorname{depth}_B M \geq 1$ and then $\delta_A(M) \geq \delta_B(M)$. Moreover, $\delta_A(M) = \delta_B(M)$ if and only if $\operatorname{length}_{\mathcal{O}} \Phi_A = \operatorname{length}_{\mathcal{O}} \Phi_B$.

Proof. Since $\mathfrak{p}_A B = \mathfrak{p}_B$ one has $I_A B \subseteq I_B$, so there is an exact sequence

$$0 \longrightarrow \frac{I_B}{I_A B} \longrightarrow \frac{B}{I_A B} \longrightarrow \frac{B}{I_B} \longrightarrow 0$$

of B-modules. Applying $\operatorname{Hom}_B(-, M)$ yields an exact sequence

$$0 \longrightarrow M[I_B] \longrightarrow M[I_A] \longrightarrow \operatorname{Hom}_B(\frac{I_B}{I_A B}, M)$$

of B-modules. Since $M[\mathfrak{p}_B] = M[\mathfrak{p}_A]$, the 1st part of the statement is immediate for the inclusion $M[I_B] \subseteq M[I_A]$ and the definition of congruence modules.

Observe that I_B/I_AB is annihilated by $\mathfrak{p}_A$ and I_A and hence it has finite length over A, so also over B. Thus, when $\operatorname{depth}_B M \geq 1$, one has $\operatorname{Hom}_B(I_B/I_AB, M) = 0$, so $M[I_B] = M[I_A]$. This gives the desired isomorphism.

The inequality of Wiles defects is clear since the map $\Phi_A \to \Phi_B$ is surjective [7, Section 5.2] as is the statement about equality. ■

4 Criteria for Freeness

In this section, we relate the freeness of a module over a local ring in $\mathsf{C}_{\mathcal{O}}$ to numerical invariants associated with its congruence module. The main result here is Theorem 4.3. In addition to the results on congruence modules presented in Section 3, its proof uses the following criterion for freeness of modules over Gorenstein local rings of Krull dimension zero.

Lemma 4.1. Let R be a Gorenstein local ring with maximal ideal $\mathfrak{m}$ and of Krull dimension zero. A finitely generated R-module M is free if and only if

$$\operatorname{length}_R M \leq \operatorname{length}_R (R[\mathfrak{m}] \cdot M) \operatorname{length} R\,.$$

Proof. The ideal $R[\mathfrak{m}]$ is the socle of the ring R and since the ring is Gorenstein and of dimension zero, one has $R[\mathfrak{m}] \cong k$; see [5, Theorem 3.2.10]. Both sides of the desired inequality are additive on direct sums of modules and coincide on R, by the remark about socles. Thus, we can assume M has no free summands. Consider the injective hull $M \subseteq F$ of M. Since R is Gorenstein of dimension zero, the only indecomposable injective module is R itself; see [5, Proposition 3.2.12(e)]. Thus, the R-module F is free, and since M has not free summands $M \subseteq \mathfrak{m}F$. Therefore,

$$R[\mathfrak{m}] \cdot M \subseteq R[\mathfrak{m}] \cdot (\mathfrak{m}F) = 0\,.$$

The hypothesis thus yields $\operatorname{length}_R M = 0$ and so $M = 0$. ■

In the sequel, we use some basic results, recalled below, from the theory of multiplicities for modules over local rings; for details see [5, Chapter 4].

Let A be a local ring with maximal ideal $\mathfrak{m}_A$ and M a finitely generated A-module. We write $e_A(M)$ for the Hilbert–Samuel multiplicity with respect to $\mathfrak{m}_A$ of the A-module M; see [5, §4.6]. For $M = A$, we write $e(A)$ instead of $e_A(A)$. Here are the crucial facts about multiplicities.

When A has Krull dimension zero, then $e_A(M) = \operatorname{length}_A M$.

When A is a finite $\mathcal{O}$-algebra, then $e_A(M) = (\operatorname{rank}_{\mathcal{O}} M)(\operatorname{rank}_{\mathcal{O}} A)$.

One has $e_A(M) \geq 0$ with strict inequality if and only if $\dim M = \dim A$. This also follows from the additivity formula (4.1) below.

Set $\Lambda := \{\mathfrak{q} \in \operatorname{Spec} A \mid \dim(A/\mathfrak{q}) = \dim A\}$; these are the prime ideals corresponding to the components of $\operatorname{Spec} A$ of maximal dimension. There is an equality

$$e_A(M) = \sum_{\mathfrak{q}\in\Lambda} (\operatorname{length}_{A_{\mathfrak{q}}} M_{\mathfrak{q}}) e(A_{\mathfrak{q}})\,. \tag{4.1}$$

In particular, if the rank of M at each $\mathfrak{q}$ in Λ is at most that at $\mathfrak{p}_A$, then

$$e_A(M) \leq (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A])(\sum_{\mathfrak{q}\in\Lambda} e(A_{\mathfrak{q}})) = (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]) \cdot e(A)\,. \tag{4.2}$$

This holds in particular when $M := B$ for any surjective map $A \twoheadrightarrow B$ in $\mathsf{C}_{\mathcal{O}}$ because one has $B_{\mathfrak{p}_A} = B_{\mathfrak{p}_B} = \mathcal{O}$, and the rank of B at any $\mathfrak{q}$ in Λ is at most one.

Lemma 4.2. Let $A \in \mathsf{C}_{\mathcal{O}}$ be a Gorenstein ring and $x \in A$ a nonzero divisor such that $\lambda_A(x)$ is a uniformizing parameter for $\mathcal{O}$. The ring $R := A/xA$ is Gorenstein with socle equal to $I_A \cdot R$.

Proof. Since $\dim A = 1$, by Lemma 2.1, the ring R is zero dimensional, with maximal ideal $\mathfrak{m}_R := \mathfrak{m}_A R$. Rees' theorem [5, Lemma 3.1.16] yields isomorphisms

$$\operatorname{Ext}^i_R(k, R) \cong \operatorname{Ext}^{i+1}_A(k, A) \quad \text{for all } i.$$

In particular, the socle $R[\mathfrak{m}_R]$ of R can be computed as follows:

$$\operatorname{Hom}_R(k, R) \cong \operatorname{Ext}^1_A(k, A) \cong \frac{I_A}{\varpi I_A} = I_A \cdot R\,.$$

The equality holds because $I_A \cap xA = xI_A = \varpi I_A$; see Lemma 3.1. This justifies the last part of the result. ■

Here is an analogue of Lemma 4.1 in the category $\mathsf{C}_{\mathcal{O}}$. By (4.2), the upper bound on $e_A(M)$ holds when the rank of M at each generic point of A is at most d. Thus, the result below contains Theorem 1.2 from the Introduction. It was suggested by the arguments in the 2nd half of the proof of [8, Theorem 2.4] to prove freeness of modules over complete intersection rings using numerical conditions. There do exist rings in $\mathsf{C}_{\mathcal{O}}$ that are Gorenstein but not complete intersection; see 2.

Theorem 4.3. Let $A \in \mathsf{C}_{\mathcal{O}}$ be a Gorenstein ring, M a finitely generated A-module with $\operatorname{depth}_A M \geq 1$, and set $d := \operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A]$. The A-module M is free if, and only if, there are inequalities

$$\delta_A(M) \leq d \cdot \delta_A(A) \qquad \text{and} \qquad e_A(M) \leq d \cdot e(A)\,.$$

Given Theorem 3.3, the inequality on the left is equivalent to $\delta_A(M) = d \cdot \delta_A(A)$.

Proof. The "only if" direct is clear. As to the converse, the hypothesis $\delta_A(M) \leq d \cdot \delta_A(A)$ is equivalent to $M[\mathfrak{p}_A] = I_A M$, by Theorem 3.3.

Pick an element $x \in A$ mapping to a uniformizer for $\mathcal{O}$ and such that x is a nonzero divisor on both A and M. This is possible as A and M have depth one. Set $R = A/xA$ and $N = M/xM$. Then R is a Gorenstein local ring of dimension zero, with maximal ideal $\mathfrak{m}_A R$ and socle $R[\mathfrak{m}_A R] = I_A R$; see Lemma 4.2. Since x is a nonzero divisor on A and M, and hence on $I_A M$, and not in $\mathfrak{m}_A^2$, one gets

$$e(A) = \operatorname{length} R\,, \quad e_A(M) = \operatorname{length}_R N \quad \text{and} \quad e_A(I_A M) = \operatorname{length}_R (I_A M / x I_A M)\,.$$

We also have the following sequence of equalities:

$$\begin{aligned}
\operatorname{length}_R (I_A R \cdot N) &= \operatorname{length}_R \frac{(I_A M + xM)}{xM} \\
&= \operatorname{length}_R \frac{I_A M}{(xM \cap I_A M)} \\
&= \operatorname{length}_R (I_A M / x I_A M)\,,
\end{aligned}$$

where the 3rd one holds by the observation recorded in Lemma 3.1, applied with $J = \mathfrak{p}_A$ to $I_A M = M[\mathfrak{p}_A]$. Observe that $e_A(I_A M) = e_A(M[\mathfrak{p}_A]) = d$, so the hypothesis on multiplicities translates to

$$\operatorname{length}_R N \leq \operatorname{length}_R (I_A R \cdot N) \operatorname{length} R\,.$$

By Lemma 4.2, the ring R is Gorenstein with socle $I_A R$, so Lemma 4.1 applies to yield the R-module N is free. Thus, the A-module M is free. ■

Theorem 4.3 implies the following known isomorphism criteria; see [9, Lemma A.8] and [7, Theorem 5.21]. We state it here for ease of reference as its needed later, and our methods yield a new proof of it.

Corollary 4.4. Let $\varphi\colon A \to B$ be a surjective map in $\mathsf{C}_{\mathcal{O}}$. The map φ is an isomorphism under either of the following conditions:

(1) $\operatorname{length}_{\mathcal{O}} \Psi_A = \operatorname{length}_{\mathcal{O}} \Psi_B$, the ring A is Gorenstein and B is Cohen–Macaulay;

(2) $\operatorname{length}_{\mathcal{O}} \Phi_A = \operatorname{length}_{\mathcal{O}} \Phi_B$ and B is complete intersection.

Proof. The goal is to deduce that B is free as an A-module, so $\operatorname{Ker}(\varphi) = 0$.

(1) Since $\Psi_B \cong \Psi_A(B)$, by Lemma 3.4, the hypothesis yields $\delta_A(B) = \delta_A(A)$. As $e_A(B) \le e(A)$ always holds—see 4—we can apply Theorem 4.3 to deduce that B is free as an A-module.

(2) Lemma 3.4 yields the 1st equality below

$$\delta_A(B) = \delta_B(B) = 0\,.$$

The 2nd one holds for B is complete intersection. Apply Theorem 4.3 again. ■

4.1 Diamond's theorem

We begin by recalling the result below from [9, Proposition A.6]; it is used in the proof of Theorem 4.6(1).

Theorem 4.5. Let $\varphi\colon A \to B$ in $\mathsf{C}_{\mathcal{O}}$ be a surjective map with $\operatorname{depth} B \ge 1$. If $\delta_A(B) = 0$, then φ is an isomorphism of complete intersections.

Given (4.2), it is immediate that the result below contains [8, Theorem 2.4], which was proved under the additional hypotheses that A is an $\mathcal{O}$-algebra and M is a finite free $\mathcal{O}$-module.

Theorem 4.6. Let A be an object in $\mathsf{C}_{\mathcal{O}}$ and M a nonzero finitely generated A-module supported at $\mathfrak{p}_A$, and with $\operatorname{depth}_A M \ge 1$.

(1) If $\delta_A(M) = 0$, then the ring A is complete intersection, M is faithful, and $M[\mathfrak{p}_A] = I_A M$.

(2) If moreover $e_A(M) \le (\operatorname{rank}_{\mathcal{O}} M[\mathfrak{p}_A])e(A)$, then the A-module M is free.

Proof. Let B denote the image of A in $\mathrm{End}_A(M)$. Since M is supported at $\mathfrak{p}_A$, the canonical surjection $A \to B$ is in $\mathsf{C}_{\mathcal{O}}$. Since M has positive depth, so does $\mathrm{End}_A(M)$, and hence also B. Thus, Lemma 3.4 applies and gives the 1st inequality below

$$\delta_A(M) \geq \delta_B(M) \geq 0\,.$$

The 2nd inequality is by Theorem 3.3 applied to B. Thus, if $\delta_A(M) = 0$, then

$$\delta_A(M) = 0 = \delta_B(M)\,.$$

The 1st equality already implies $M[\mathfrak{p}_A] = I_A M$, by Theorem 3.3. The equality of defects of M over A and B yields that the natural map $\Phi_A \to \Phi_B$ is an isomorphism; see Lemma 3.4. This gives the 1st equality below:

$$\mathrm{length}_{\mathcal{O}}\, \Phi_A = \mathrm{length}_{\mathcal{O}}\, \Phi_B = \mathrm{length}_{\mathcal{O}}\, \Psi_B\,.$$

Since $\delta_B(M) = 0$, applying Theorem 3.3 but now to M viewed as a B-module gives $\delta_B(B) = 0$, which justifies the 2nd equality. Since $\operatorname{depth} B \geq 1$, the map $A \to B$ is an isomorphism of complete intersections; see Theorem 4.5. In particular, the A-module M is faithful.

This completes the proof of the 1st statement. Given this, the 2nd part is immediate from Theorem 4.3. ■

4.2 An analog of Wiebe's result for modules

Wiles' theorem characterizing complete intersection rings $A \in \mathsf{C}_{\mathcal{O}}$ can be deduced from the theorem of Wiebe [5, Theorem 2.3.16] that when R is a local ring with maximal ideal $\mathfrak{m}$, its Fitting ideal $\mathrm{Fitt}_R(\mathfrak{m})$ is nonzero if and only if R is a complete intersection of dimension zero. Diamond's theorem suggests the following module theoretic extension of Wiebe's theorem; compare with Lemma 4.1.

Lemma 4.7. Let R be a noetherian local ring, with maximal ideal $\mathfrak{m}$. If M is a nonzero finitely generated R-module such that

$$e(M) \leq \mathrm{length}_R\,(\mathrm{Fitt}_R(\mathfrak{m}) \cdot M) \cdot e(R)\,,$$

then R is a complete intersection with $\dim R = 0$, and M is free.

Proof. As M is nonzero, $e(M) \neq 0$ so the hypothesis implies $\mathrm{Fitt}_R(\mathfrak{m})$ is nonzero. Thus, Wiebe's theorem [5, Theorem 2.3.16] implies R is complete intersection of Krull dimension zero. Moreover, $\mathrm{Fitt}_R(\mathfrak{m}) = R[\mathfrak{m}]$, the socle of R. At this point, we can invoke Lemma 4.1 to deduce that M is free. ■

5 Venkatesh's Formula

In this section, we establish a formula for the defect of a local ring in $\mathsf{C}_{\mathcal{O}}$, in terms of certain André–Quillen homology modules, see Theorem 5.2. This gives a different proof of a variant of the results in [16] and [10].

Throughout this section, fix A in $\mathsf{C}_{\mathcal{O}}$ with $\dim A = 1$, and let

$$A \to B := A/\Gamma_{\mathfrak{m}_A}(A)$$

be the maximal Cohen–Macaulay quotient of A; here $\Gamma_{\mathfrak{m}_A}(A)$ is the $\mathfrak{m}_A$-power torsion submodule of A.

Proposition 5.1. Let $\alpha\colon C \to A$ be a surjective map in $\mathsf{C}_{\mathcal{O}}$, with C a Gorenstein ring, and set $I := \lambda_C(\mathrm{ann}_C(\mathrm{Ker}\,\alpha))$. With B as above, one has an equality

$$\mathrm{length}_{\mathcal{O}}\, \Psi_C = \mathrm{length}_{\mathcal{O}}\, \Psi_B + \mathrm{length}_{\mathcal{O}}\, (\mathcal{O}/I)\,.$$

Proof. First, we reduce to the case $A = B$. Applying $\mathrm{Hom}_C(-, C)$ to the exact sequence

$$0 \longrightarrow \Gamma_{\mathfrak{m}_A}(A) \longrightarrow A \longrightarrow B \longrightarrow 0$$

yields an exact sequence

$$0 \longrightarrow \mathrm{Hom}_C(B, C) \longrightarrow \mathrm{Hom}_C(A, C) \longrightarrow \mathrm{Hom}_C(\Gamma_{\mathfrak{m}_A}(A), C) = 0$$

where the equality on the right holds because $\mathrm{depth}\, C \geq 1$. This gives the equality

$$\mathrm{Hom}_C(B, C) = \mathrm{Hom}_C(A, C)\,,$$

so that we can replace A by B and assume A is Cohen–Macaulay.

Consider the exact sequence

$$0 \longrightarrow \mathrm{Ker}\,\alpha \longrightarrow C \longrightarrow A \longrightarrow 0\,.$$

Applying $\operatorname{Hom}_C(\mathcal{O},-)$ to it yields the exact sequence of $\mathcal{O}$-modules

$$0 \longrightarrow \operatorname{Hom}_C(\mathcal{O}, \operatorname{Ker}\alpha) \longrightarrow \operatorname{Hom}_C(\mathcal{O}, C) \longrightarrow \operatorname{Hom}_C(\mathcal{O}, A) \longrightarrow \operatorname{Ext}^1_C(\mathcal{O}, \operatorname{Ker}\alpha) \longrightarrow 0.$$

Since the map $C \to \mathcal{O}$ factors through A one has $\operatorname{Ker}\alpha \subseteq \mathfrak{p}_C$ so

$$\operatorname{Hom}_C(\mathcal{O}, \operatorname{Ker}\alpha) = I_C \cap \operatorname{Ker}\alpha \;\subseteq\; I_C \cap \mathfrak{p}_C = 0\,.$$

Moreover, $\operatorname{Hom}_C(\mathcal{O}, A) = \operatorname{Hom}_A(\mathcal{O}, A)$ so the exact sequence above becomes

$$0 \longrightarrow \eta_C \longrightarrow \eta_A \longrightarrow \operatorname{Ext}^1_C(\mathcal{O}, \operatorname{Ker}\alpha) \longrightarrow 0\,,$$

where η_C and η_A are the images of I_C and I_A in $\mathcal{O}$. Thus, we get an exact sequence

$$0 \longrightarrow \operatorname{Ext}^1_C(\mathcal{O}, \operatorname{Ker}\alpha) \longrightarrow \Psi_C \longrightarrow \Psi_A \longrightarrow 0\,,$$

and hence the equality

$$\operatorname{length}_{\mathcal{O}} \Psi_C = \operatorname{length}_{\mathcal{O}} \Psi_A + \operatorname{length}_{\mathcal{O}} \operatorname{Ext}^1_C(\mathcal{O}, \operatorname{Ker}\alpha)\,. \tag{5.1}$$

Now we analyze the Ext term above. For this, it is convenient to work in the stable module category of C; see [6] for background. Since $\mathcal{O}$ is maximal Cohen–Macaulay as a C-module, [6, Corollary 6.4.1] gives the 1st isomorphism below:

$$\operatorname{Ext}^1_C(\mathcal{O}, \operatorname{Ker}\alpha) \cong \underline{\operatorname{Hom}}_C(\mathcal{O}, \Omega^{-1} \operatorname{Ker}\alpha) \cong \underline{\operatorname{Hom}}_C(\mathcal{O}, A).$$

The 2nd isomorphism arises from the exact sequence $0 \to \operatorname{Ker}\alpha \to C \to A \to 0$. On the other hand, keeping in mind that A is also maximal Cohen–Macaulay as a C-module, from Auslander duality [6, Theorem 7.7.5] one gets that

$$\operatorname{length}_{\mathcal{O}} \underline{\operatorname{Hom}}_C(\mathcal{O}, A) = \operatorname{length}_{\mathcal{O}} \underline{\operatorname{Hom}}_C(A, \mathcal{O})\,.$$

By the definition of stable homomorphism, one has the exact sequence in the top row of the diagram below:

$$\begin{tikzcd}
\operatorname{Hom}_C(A, C) \otimes_C \mathcal{O} \arrow[r] \arrow[d, equal] & \operatorname{Hom}_C(A, \mathcal{O}) \arrow[r] \arrow[d, "\cong"] & \underline{\operatorname{Hom}}_C(A, \mathcal{O}) \arrow[r] \arrow[d] & 0 \\
\operatorname{ann}_C(\operatorname{Ker}\alpha) \otimes_C \mathcal{O} \arrow[r] & \mathcal{O} \arrow[r] & \underline{\operatorname{Hom}}_C(A, \mathcal{O}) \arrow[r] & 0
\end{tikzcd}$$

Thus, $\underline{\mathrm{Hom}}_C(A,\mathcal{O}) \cong \mathcal{O}/I$. Combining with this (5.1) yields the desired equality. ■

Let now $\alpha\colon C \to A$ be a surjective map in $\mathsf{C}_{\mathcal{O}}$ with C a complete intersection; see [9, Lemma A.7]. We say that such an α is *minimal* if the natural map $\Phi_C \to \Phi_A$ is bijective; it is always surjective. It is helpful to introduce the ideals

$$I := \lambda_C(\mathrm{ann}_C(\mathrm{Ker}\,\alpha)) \qquad \text{and} \qquad J := \lambda_C(\mathrm{Fitt}_C(\mathrm{Ker}\,\alpha))\,.$$

In particular, $I \supseteq J$.

Given a map of rings $A \to B$ and a B-module M, we write $\mathrm{D}_i(B/A;M)$ for the ith André–Quillen homology module of the A-algebra B, with coefficients in M. We only need these functors for $i = 0,1,2$ and Jacobi–Zariski sequence associated to maps; see, for instance, [4, §2], or [12].

Here is a formula for $\delta_A(B)$ in terms of these modules; it can also be expressed as an equality of Fitting ideals. See 5 for connections with earlier work.

Theorem 5.2. With notation as above, one has (in)equalities

$$\delta_A(B) = \mathrm{length}_{\mathcal{O}}\,\mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) - \mathrm{length}_{\mathcal{O}}\,(I/J) \le \mathrm{length}_{\mathcal{O}}\,(\mathcal{O}/I)\,.$$

Moreover, equality holds on the right when α is minimal.

Proof. Since $\mathrm{D}_1(A/C;\mathcal{O}) = (\mathrm{Ker}\,\alpha)\otimes_C \mathcal{O}$, one gets an equality

$$\mathrm{length}_{\mathcal{O}}\,\mathrm{D}_1(A/C;\mathcal{O}) = \mathrm{length}_{\mathcal{O}}\,(\mathcal{O}/J)\,.$$

From this and the Jacobi–Zariski sequence associated to $C \to A \to \mathcal{O}$, which reads

$$0 \to \mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) \to \mathrm{D}_1(A/C;\mathcal{O}) \to \Phi_C \longrightarrow \Phi_A \to 0\,,$$

one gets equalities

$$\begin{aligned}\mathrm{length}_{\mathcal{O}}\,\Phi_A - \mathrm{length}_{\mathcal{O}}\,\Phi_C &= \mathrm{length}_{\mathcal{O}}\,\mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) - \mathrm{length}_{\mathcal{O}}\,\mathrm{D}_1(A/C;\mathcal{O})\\ &= \mathrm{length}_{\mathcal{O}}\,\mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) - \mathrm{length}_{\mathcal{O}}\,(\mathcal{O}/J)\,.\end{aligned}$$

In particular, $\mathrm{length}_{\mathcal{O}}\,\mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) - \mathrm{length}_{\mathcal{O}}\,(\mathcal{O}/J) \le 0$ with equality when α is minimal; this justifies the inequality and the last assertion in the statement of the theorem.

Moreover, the equality above yields the 2nd equality below:

$$\begin{aligned}\operatorname{length}_{\mathcal{O}}\Phi_A - \operatorname{length}_{\mathcal{O}}\Psi_B &= \operatorname{length}_{\mathcal{O}}\Phi_A - \operatorname{length}_{\mathcal{O}}\Phi_C + \operatorname{length}_{\mathcal{O}}(\mathcal{O}/I)\\ &= \operatorname{length}_{\mathcal{O}}\mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) - \operatorname{length}_{\mathcal{O}}(\mathcal{O}/J) + \operatorname{length}_{\mathcal{O}}(\mathcal{O}/I)\\ &= \operatorname{length}_{\mathcal{O}}\mathrm{D}_2(\mathcal{O}/A;\mathcal{O}) - \operatorname{length}_{\mathcal{O}}(I/J)\,.\end{aligned}$$

The 1st one is by Proposition 5.1; it applies as complete intersections rings are Gorenstein, and also $\operatorname{length}_{\mathcal{O}}\Phi_C = \operatorname{length}_{\mathcal{O}}\Psi_C$. The claim about the defect of B as a A-module follows. ■

Suppose that A is a finite $\mathcal{O}$-algebra, with $\lambda\colon A \to \mathcal{O}$ a map of $\mathcal{O}$-algebras. Then it is immediate from the Jacobi–Zariski sequence associated to the map $\mathcal{O} \to A \to \mathcal{O}$ that for any integer i one has an isomorphism

$$\mathrm{D}_i(A/\mathcal{O};\mathcal{O}) \cong \mathrm{D}_{i+1}(\mathcal{O}/A;\mathcal{O})\,.$$

Let K be the field of fractions of $\mathcal{O}$, so that the $\mathcal{O}$-module $K/\mathcal{O}$ is the injective hull of the residue field of $\mathcal{O}$. Then it follows from Matlis duality [5, §3.2] that

$$\operatorname{length}_{\mathcal{O}}\mathrm{D}_i(A/\mathcal{O};\mathcal{O}) \cong \operatorname{length}_{\mathcal{O}}\mathrm{D}^i(A/\mathcal{O};K/\mathcal{O})$$

where the module on the right is the ith André–Quillen cohomology of the $\mathcal{O}$-algebra A, with coefficients in $K/\mathcal{O}$. Thus, one can rewrite the equality in Theorem 5.2 as

$$\operatorname{length}_{\mathcal{O}}\Phi_A - \operatorname{length}_{\mathcal{O}}\Psi_A(B) = \operatorname{length}_{\mathcal{O}}\mathrm{D}^1(A/\mathcal{O};K/\mathcal{O}) - \operatorname{length}_{\mathcal{O}}(I/J).$$

It is in this form that the formula was proposed by Venkatesh [16], and proved in [10]. From our perspective, the avatar in terms of André–Quillen homology is more natural.

Theorem 5.2 expresses the defect of A as a difference of two positive integers. It is not clear why they are both zero when the defect is zero, as asserted by Wiles' Theorem 4.5. What is more Venkatesh's formula only applies when $\dim A = 1$. So we sketch an argument that deduces the latter result from the former, though only under the additional hypothesis that $\dim B = 1$.

Proof of Theorem 4.5 when $\dim B = 1$. We start by reducing to the case where $\dim A = 1$. Set $\mathfrak{b} = \operatorname{Ker}(A \to B)$ and $A' := A/\mathfrak{b}^2$. Thus, the map φ factors through the surjection $A \to A'$. This gives the second of the following inequalities:

$$\operatorname{length}_{\mathcal{O}} \Psi_{B'} \geq \operatorname{length}_{\mathcal{O}} \Phi_A \geq \operatorname{length}_{\mathcal{O}} \Phi_{A'}\,.$$

The 1st one is by hypothesis. Thus, the hypothesis of the desired result applies to the surjection $A' \to B$; we claim it suffices to verify the conclusion for this map, for if this map is an isomorphism one gets that $\mathfrak{b} = \mathfrak{b}^2$, so that $\mathfrak{b} = 0$, that is to say φ is an isomorphism, as desired. Since $\dim A' = \dim B$, we can replace A by A' and assume $\dim A = 1$.

Next we reduce to the case where B is A modulo its $\mathfrak{m}_A$-power torsion ideal, so we can apply Venkatesh's equality: set $B' := A/\Gamma_{\mathfrak{m}_A}(A)$. Since φ is surjective, $\varphi(\mathfrak{m}_A) = \mathfrak{m}_B$ so that $\varphi(\Gamma_{\mathfrak{m}_A}(A))$ is $\mathfrak{m}_B$-power torsion; thus $\operatorname{depth} B \geq 1$ implies $\varphi(\Gamma_{\mathfrak{m}_A}(A)) = 0$, that is to say, φ factors through the surjection $A \to B'$. This gives the 1st inequality below:

$$\operatorname{length}_{\mathcal{O}} \Psi_{B'} \geq \operatorname{length}_{\mathcal{O}} \Psi_B \geq \operatorname{length}_{\mathcal{O}} \Phi_A\,.$$

The 2nd one is part of the hypothesis. Since $\operatorname{depth} B' \geq 1$ as well, the map $A \to B'$ also satisfies the hypothesis of the desired result. We claim that it suffices to verify then that A is complete intersection. Indeed then $A = B'$ and keeping in mind that the lengths of Ψ_A and Φ_A coincide, we get the inequality:

$$\operatorname{length}_{\mathcal{O}} \Psi_B \geq \operatorname{length}_{\mathcal{O}} \Psi_A\,.$$

Then Corollary 4.4 applies to yield that φ is an isomorphism. Thus, we can assume $B = B'$, which puts us in the context of Theorem 5.2.

Since $\dim A = 1$, we can choose a minimal presentation $\alpha\colon C \to A$, with C a complete intersection; see 5. Theorem 5.2 with $M = B$ yields

$$\operatorname{length}_{\mathcal{O}} \Phi_A - \operatorname{length}_{\mathcal{O}} \Psi_B = \operatorname{length}_{\mathcal{O}} (\mathcal{O}/I)\,.$$

By the hypothesis, the term on the left is negative so we deduce that $I = \mathcal{O}$. Therefore, $\operatorname{Ker} \alpha = 0$, so $A = C$ and A is complete intersection. ■

Funding

This work was supported by the National Science Foundation [DMS-200985 to S.B.I.].

Acknowledgments

It is a pleasure to thank a referee for a careful reading of the manuscript.

References

[1] Avramov, L. L. and S. Iyengar. "Homological Criteria for Regular Homomorphisms and for Locally Complete Intersection Homomorphisms." In *Algebra, Arithmetic and Geometry, Part I, II, Mumbai, 2000*. Tata Inst. Fund. Res. Stud. Math. 16. Bombay: Tata Inst. Fund. Res., 2002, pp. 97–122.

[2] Böckle, G., C. B. Khare, and J. Manning. "Wiles defect for Hecke algebras that are not complete intersections." *Compos. Math.* 157, no. 9 (2021): 2046–88. 0010-437X, MR 4301563. http://10.1112/S0010437X21007454.

[3] Böckle, G., C. B. Khare, and J. Manning. "Wiles defect of Hecke algebras via local-global arguments." (2021): preprint https://arxiv.org/abs/2108.09729.

[4] Brochard, S., S. B. Iyengar, and C. B. Khare. "A freeness criterion without patching for modules over local rings." *J. Inst. Math. Jussieu* (2021): 1–13. http://10.1017/S147474802100061X.

[5] Bruns, W. and J. Herzog. *Cohen-Macaulay Rings*. Cambridge: Cambridge University Press, 1998. xiv+453.

[6] Buchweitz, R.-O. "Maximal Cohen-Macaulay Modules and Tate Cohomology." In *Maximal Cohen–Macaulay Modules and Tate Cohomology*, vol. 262. Providence, RI: American Mathematical Society, 2021.

[7] Darmon, H., F. Diamond, and R. Taylor. "Fermat's Last Theorem." In *Elliptic Curves, Modular Forms & Fermat's Last Theorem, Hong Kong, 1993*, pp. 2–140. Cambridge, MA: Int. Press, 1997.

[8] Diamond, F. "The Taylor-Wiles construction and multiplicity one." *Invent. Math.* 128, no. 2 (1997): 379–91.

[9] Fakhruddin, N., C. Khare, and R. Ramakrishna. "Quantitative level lowering for Galois representations." *J. Lond. Math. Soc. (2)* 103, no. 1 (2021): 250–87.

[10] Fakhruddin, N. and C. B. Khare. "A formula of Venkatesh." (2021): preprint.

[11] Hida, H. "On congruence divisors of cusp forms as factors of the special values of their zeta functions." *Invent. Math.* 64, no. 2 (1981): 221–62.

[12] Iyengar, S. "André-Quillen Homology of Commutative Algebras." In *Interactions Between Homotopy Theory and Algebra*, vol. 436. Providence, RI: Amer. Math. Soc., 2007, pp. 203–34.

[13] Lenstra, Jr., H. W. "Complete Intersections and Gorenstein Rings." In *Elliptic Curves, Modular Forms, & Fermat's Last Theorem, Hong Kong, 1993, Ser. Number Theory, I*, pp. 99–109. Cambridge, MA: Int. Press, 1995.

[14] Ribet, K. A. "Modp Hecke operators and congruences between modular forms." *Invent. Math.* 71, no. 1 (1983): 193–205.

[15] Taylor, R. and A. Wiles. "Ring-theoretic properties of certain Hecke algebras." *Ann. of Math. (2)* 141, no. 3 (1995): 553–72.

[16] Venkatesh, A. “Derived version of Wiles’s equality.” (2016): preprint.

[17] Wiles, A. “Modular elliptic curves and Fermat’s last theorem.” *Ann. of Math. (2)* 141, no. 3 (1995): 443–551.