Contemporary Mathematics

On the arithmetic rank of certain Segre products

Anurag K. Singh and Uli Walther

Abstract. We compute the arithmetic ranks of the defining ideals of homogeneous coordinate rings of certain Segre products arising from elliptic curves. The cohomological dimension of these ideals varies with the characteristic of the field, though the arithmetic rank does not. We also study the related set-theoretic Cohen-Macaulay property for these ideals.

In [**12**] Lyubeznik writes: *Part of what makes the problem about the number of defining equations so interesting is that it can be very easily stated, yet a solution, in those rare cases when it is known, usually is highly nontrivial and involves a fascinating interplay of Algebra and Geometry.*

In this note we present one of these rare cases where a solution is obtained: for a smooth elliptic curve $E \subset \mathbb{P}^2$, we determine the arithmetic rank of the ideal $\mathfrak{a}$ defining the Segre embedding $E \times \mathbb{P}^1 \subset \mathbb{P}^5$, and exhibit a natural generating set for $\mathfrak{a}$ up to radical. The ideal $\mathfrak{a}$ is not a set-theoretic complete intersection and, in the case of characteristic zero, we use reduction modulo p methods to prove moreover that $\mathfrak{a}$ is not set-theoretically Cohen-Macaulay.

1. The Segre embedding of $E \times \mathbb{P}^1$

Let A and B be $\mathbb{N}$-graded rings over a field $A_0 = B_0 = K$. The *Segre product* of A and B is the ring

$$A\#B = \bigoplus_{n \geq 0} A_n \otimes_K B_n$$

which is a subring, in fact a direct summand, of the tensor product $A \otimes_K B$. The ring $A\#B$ has a natural $\mathbb{N}$-grading in which $(A\#B)_n = A_n \otimes_K B_n$. If $U \subset \mathbb{P}^r$ and $V \subset \mathbb{P}^s$ are projective varieties with homogeneous coordinate rings A and B respectively, then the Segre product $A\#B$ is a homogeneous coordinate ring for the Segre embedding $U \times V \subset \mathbb{P}^{rs+r+s}$.

Let E be a smooth elliptic curve over a field K. Then E can be embedded in $\mathbb{P}^2$, and so $E = \operatorname{Proj}(K[x_0, x_1, x_2]/(f))$ where f is a homogeneous cubic polynomial.

1991 *Mathematics Subject Classification.* Primary 13C40, 14M10; Secondary 13D45, 14B15.
Key words and phrases. Local cohomology, Segre products, arithmetic rank.
The first author is supported in part by the NSF under Grant DMS 0300600.
The second author is supported in part by the NSF under Grant DMS 0100509.

The Segre product $E \times \mathbb{P}^1$ has an embedding in $\mathbb{P}^5$ with homogeneous coordinate ring

$$S = \frac{K[x_0, x_1, x_2]}{(f)} \ \# \ K[y_0, y_1],$$

i.e., S is the subring of $K[x_0, x_1, x_2, y_0, y_1]/(f)$ generated by the six monomials $x_i y_j$ for $0 \le i \le 2$ and $0 \le j \le 1$. The relations amongst these generators arise from the equations

$$x_i y_j \cdot \ x_k y_l = x_i y_l \cdot \ x_k y_j$$

defining $\mathbb{P}^2 \times \mathbb{P}^1 \subset \mathbb{P}^5$, and the four equations

$$y_0^{3-k} y_1^k f(x_0, x_1, x_2) = 0 \quad \text{for} \quad 0 \le k \le 3.$$

The ring S is normal since it is a direct summand of a normal ring. The local cohomology of S with support at its homogeneous maximal ideal $\mathfrak{m}$ may be computed by the Künneth formula, which shows that $H^2_{\mathfrak{m}}(S)$ is isomorphic to

$$[H^2_{\mathfrak{m}}(S)]_0 = H^1(E, \mathcal{O}_E) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}) = K.$$

In particular, S is a normal domain of dimension 3 which is not Cohen-Macaulay.

Let $R = K[z_{ij} : 0 \le i \le 2,\ 0 \le j \le 1]$ be a polynomial ring. Then R has a K-algebra surjection onto S where

$$z_{ij} \mapsto x_i y_j.$$

We use f_{x_i} to denote the partial derivative of $f(x_0, x_1, x_2)$ with respect to x_i. The Euler identity implies that

$$3f(x_0, x_1, x_2) = \sum_{i=0}^{2} x_i f_{x_i}(x_0, x_1, x_2),$$

and multiplying by $y_0^2 y_1$ and $y_0 y_1^2$ we obtain, respectively, the equations

$$3y_0^2 y_1 f(x_0, x_1, x_2) = \sum_{i=0}^{2} z_{i1} f_{x_i}(z_{00}, z_{10}, z_{20})$$

and

$$3y_0 y_1^2 f(x_0, x_1, x_2) = \sum_{i=0}^{2} z_{i0} f_{x_i}(z_{01}, z_{11}, z_{21}).$$

Consequently if K is a field of characteristic other than 3, then the kernel of the surjection $R \longrightarrow S$ is the ideal $\mathfrak{a}$ generated by the seven polynomials $z_{10}z_{21} - z_{20}z_{11}$, $z_{20}z_{01} - z_{00}z_{21}$, $z_{00}z_{11} - z_{10}z_{01}$, and

$$\sum_{i=0}^{2} z_{is} f_{x_i}(z_{0t}, z_{1t}, z_{2t}), \quad \text{where} \quad 0 \le s, t \le 1.$$

We prove that the ideal $\mathfrak{a}$ has arithmetic rank four, and that the last four polynomials above generate $\mathfrak{a}$ up to radical:

Theorem 1.1. *Let $E = \operatorname{Proj}(K[x_0, x_1, x_2]/(f))$ be a smooth elliptic curve and let $\mathfrak{a} \subset R = K[z_{ij} : 0 \le i \le 2,\ 0 \le j \le 1]$ be the defining ideal of the homogeneous coordinate ring of the Segre embedding $E \times \mathbb{P}^1 \subset \mathbb{P}^5$. If the characteristic of the field K does not equal 3, then the arithmetic rank of the ideal $\mathfrak{a}$ is 4 and*

$$\mathfrak{a} = \operatorname{rad}\left(R \sum_{i=0}^{2} z_{is} f_{x_i}(z_{0t}, z_{1t}, z_{2t}) : 0 \le s, t \le 1 \right).$$

Proof. Let $(p_0, p_1, p_2, q_0, q_1, q_2) \in \mathbb{A}^6$ be a root of the four polynomials above which, we claim, generate $\mathfrak{a}$ up to radical. Then

$$\begin{gathered} f(p_0,p_1,p_2) = 0, \\ q_0 f_{x_0}(p_0,p_1,p_2) + q_1 f_{x_1}(p_0,p_1,p_2) + q_2 f_{x_2}(p_0,p_1,p_2) = 0, \\ p_0 f_{x_0}(q_0,q_1,q_2) + p_1 f_{x_1}(q_0,q_1,q_2) + p_2 f_{x_2}(q_0,q_1,q_2) = 0, \\ f(q_0,q_1,q_2) = 0. \end{gathered}$$

We claim that the size two minors of the matrix

$$\begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \end{pmatrix}$$

must be zero. If not, then $P = (p_0, p_1, p_2)$ and $Q = (q_0, q_1, q_2)$ are distinct points of $\mathbb{P}^2$. The first and fourth equations imply that the points P and Q lie on the elliptic curve $E \subset \mathbb{P}^2$. The second equation implies that Q lies on the tangent line to E at point P, and similarly the third equation implies that P lies on the tangent line to E at Q. But then the secant line joining P and Q meets the elliptic curve with multiplicity 4, which is not possible. Alternatively, consider the group law on E using an inflection point as the identity element of the group. Then the second and third equations imply that $2P+Q = 0 = P+2Q$ in the group law, and so P and Q are the same point of $\mathbb{P}^2$. This proves the claim, and it follows that $(p_0, p_1, p_2, q_0, q_1, q_2) \in \mathbb{A}^6$ is a zero of all polynomials in the ideal $\mathfrak{a}$. By Hilbert's Nullstellensatz, $\mathfrak{a}$ is generated by the four polynomials up to radical once we tensor with $\overline{K}$, the algebraic closure of K. Since $\overline{K}$ is faithfully flat over K, the same is true over K as well and, in particular, $\operatorname{ara} \mathfrak{a} \leq 4$.

Since the ideal $\mathfrak{a}$ has height 3, the proof of the theorem will be complete once we show that $\operatorname{ara} \mathfrak{a} \neq 3$. In the next section we use étale cohomology to prove, more generally, that the defining ideal of any projective embedding of $E \times \mathbb{P}^1$ is not a set-theoretic complete intersection, Theorem 2.4. However, in characteristic 0, we can moreover show that the local cohomology module $H^4_{\mathfrak{a}}(R)$ is nonzero, from which it follows that $\operatorname{ara} \mathfrak{a} \geq 4$. (In positive characteristic, $H^4_{\mathfrak{a}}(R) = 0$ if the elliptic curve E is supersingular.) We proceed with the characteristic zero case, and our main tool here is the connection between the local cohomology modules supported at $\mathfrak{a}$, and topological information about the affine variety defined by $\mathfrak{a}$.

If $\operatorname{ara} \mathfrak{a} = 3$, then each of the 7 generators of $\mathfrak{a}$ has a power belonging to an ideal $(g_1, g_2, g_3)R \subseteq \mathfrak{a}$. This gives us seven equations, each with finitely many coefficients, and hence we may replace K by the extension of $\mathbb{Q}$ obtained be adjoining these finitely many coefficients. A finitely generated field extension of $\mathbb{Q}$ can be identified with a subfield of $\mathbb{C}$, and so it suffices to prove the desired result in the case $K = \mathbb{C}$.

Let U be the complement of $X = E \times \mathbb{P}^1$ in $\mathbb{P}^5$ and let $V \subset \mathbb{A}^6$ be the cone over U. The de Rham cohomology of V can be computed from the Čech-de Rham complex [**1**, Chapter II] corresponding to any affine cover of V. The de Rham functor on an n-dimensional affine smooth variety, when applied to any module, can only produce cohomology up to degree n (in our case, $n = 5$). It follows that the de Rham cohomology of V will be zero beyond the sum of n and the index t of the highest nonvanishing local cohomology module $H^t_{\mathfrak{a}}(R)$.

On the other hand, there is a Leray spectral sequence, [**1**, Thm. 14.18],

$$H^i_{dR}(U; \mathcal{H}^j_{dR}(\mathbb{C}^*; \mathbb{C})) \Longrightarrow H^{i+j}_{dR}(V; \mathbb{C})$$

corresponding to the fibration $V \to U$ with fiber $\mathbb{C}^*$. Since U arises through the removal of a variety of codimension two from the simply connected space $\mathbb{P}^5$, it follows that U is simply connected as well. Hence in the above spectral sequence the local coefficients are in fact constant coefficients. The nonzero terms in the E_2-page of the spectral sequence have $j = 0, 1$. Hence if k denotes the index of the top nonzero de Rham cohomology group of V, then $k-1$ is the index of the top nonzero de Rham cohomology group of U and $H^{k-1}_{dR}(U;\mathbb{C}) \cong H^k_{dR}(V;\mathbb{C})$.

We now claim that $H^8_{dR}(U;\mathbb{C})$ in nonzero. Note that $H^1_{dR}(E;\mathbb{C}) \cong \mathbb{C}^2$, so the Künneth formula gives $H^1_{dR}(X;\mathbb{C}) \cong \mathbb{C}^2$. Since sheaf and de Rham cohomology agree, using Alexander duality [**10**, V.6.6] and the compactness of X, we obtain $H^{2\cdot 5-1}_X(\mathbb{P}^5;\mathbb{C}) \cong \mathbb{C}^2$. There is a long exact sequence of sheaf cohomology

$$\cdots \longrightarrow H^i(U;\mathbb{C}) \longrightarrow H^{i+1}_X(\mathbb{P}^5;\mathbb{C}) \longrightarrow H^{i+1}(\mathbb{P}^5;\mathbb{C}) \longrightarrow \cdots,$$

which, since $H^9(\mathbb{P}^5;\mathbb{C}) = 0$, implies that $H^8(U;\mathbb{C}) \neq 0$. It follows that $H^9(V;\mathbb{C})$ is nonzero as well, and so the local cohomology module $H^4_{\mathfrak{a}}(R)$ must be nonzero. $\square$

2. Elliptic curves in positive characteristic

Let R be a ring of prime characteristic. We say that R is *F-pure* if the Frobenius homomorphism $F : R \longrightarrow R$ is pure, i.e., if $F \otimes 1_M : R \otimes_R M \longrightarrow R \otimes_R M$ is injective for all R-modules M. By [**8**, Proposition 6.11], a local ring $(R, \mathfrak{m}, K)$ is F-pure if and only if the map

$$F \otimes 1_{E_R(K)} : R \otimes_R E_R(K) \longrightarrow R \otimes_R E_R(K)$$

is injective where $E_R(K)$ is the injective hull of the residue field K.

Let E be a smooth elliptic curve over a field K of characteristic $p > 0$. The Frobenius induces a map

$$F : H^1(E, \mathcal{O}_E) \longrightarrow H^1(E, \mathcal{O}_E)$$

on the one-dimensional cohomology group $H^1(E, \mathcal{O}_E)$. The elliptic curve E is *supersingular* (or has *Hasse invariant* 0) if the map F above is zero, and is *ordinary* (*Hasse invariant* 1) otherwise. If $E = \operatorname{Proj} A$, then the map F above is precisely the action of the Frobenius on the socle of the injective hull of the residue field of A, and hence E is ordinary if and only if A is an F-pure ring.

Let $f \in \mathbb{Z}[x_0, x_1, x_2]$ be a cubic polynomial defining a smooth elliptic curve $E_\mathbb{Q} \subset \mathbb{P}^2_\mathbb{Q}$. Then the Jacobian ideal of f is (x_0, x_1, x_2)-primary in $\mathbb{Q}[x_0, x_1, x_2]$. Hence after localizing at an appropriate nonzero integer u, the Jacobian ideal of f in $\mathbb{Z}[u^{-1}][x_0, x_1, x_2]$ contains high powers of x_0, x_1, and x_2. Consequently, for all but finitely many prime integers p, the polynomial $f \mod p$ defines a smooth elliptic curve $E_p \subset \mathbb{P}^2_{\mathbb{Z}/p}$. If the elliptic curve $E_\mathbb{C} \subset \mathbb{P}^2_\mathbb{C}$ has complex multiplication, then it is a classical result [**3**] that the *density* of the supersingular prime integers p, i.e.,

$$\lim_{n\to\infty} \frac{|\{p \text{ prime} : p \le n \text{ and } E_p \text{ is supersingular}\}|}{|\{p \text{ prime} : p \le n\}|}$$

is $1/2$, and that this density is 0 if $E_\mathbb{C}$ does not have complex multiplication. However, even if $E_\mathbb{C}$ does not have complex multiplication, the set of supersingular primes is infinite by [**5**]. It is conjectured that if $E_\mathbb{C}$ does not have complex multiplication, then the number of supersingular primes less than n grows asymptotically like $C(\sqrt{n}/\log n)$, where C is a positive constant, [**11**].

Hartshorne and Speiser observed that the cohomological dimension of the defining ideal of $E_p \times \mathbb{P}^1_{\mathbb{Z}/p}$ varies with the prime p, [**7**, Example 3, p. 75]. Their arguments use the notion of F-depth, and we would like to point out how their results also follow from a recent theorem of Lyubeznik:

THEOREM 2.1. [**14**, Theorem 1.1] *Let $(R, \mathfrak{m})$ be a regular local ring containing a field of positive characteristic, and $\mathfrak{a}$ be an ideal of R. Then $H^i_{\mathfrak{a}}(R) = 0$ if and only if there exists an integer $e \geq 1$ such that $F^e : H^{\dim R - i}_{\mathfrak{m}}(R/\mathfrak{a}) \longrightarrow H^{\dim R - i}_{\mathfrak{m}}(R/\mathfrak{a})$ is the zero map, where F^e denotes the e-th iteration of the Frobenius morphism.*

COROLLARY 2.2. *Let $f \in \mathbb{Z}[x_0, x_1, x_2]$ be a cubic polynomial defining a smooth elliptic curve $E_{\mathbb{Q}} \subset \mathbb{P}^2_{\mathbb{Q}}$, and let $\mathfrak{a} \subset R = \mathbb{Z}[z_{ij} : 0 \leq i \leq 2,\ 0 \leq j \leq n]$ be the ideal defining the Segre embedding $E \times \mathbb{P}^n \subset \mathbb{P}^{3n+2}$. Then*

$$\operatorname{cd}(R/pR, \mathfrak{a}) = \begin{cases} 2n+1 & \textit{if} \quad E_p \textit{ is supersingular,} \\ 3n+1 & \textit{if} \quad E_p \textit{ is ordinary.} \end{cases}$$

PROOF. The ring $R/(\mathfrak{a} + pR)$ may be identified with the Segre product $A\#B$ where

$$A = \mathbb{Z}/p\mathbb{Z}[x_0, x_1, x_2]/(f) \quad \text{and} \quad B = \mathbb{Z}/p\mathbb{Z}[y_0, \dots, y_n].$$

Let p be a prime for which E_p is smooth, in which case the ring $A \otimes_{\mathbb{Z}/p} B$ and hence its direct summand $A\#B$ are normal. For $k \geq 1$ the Künneth formula gives us

$$\begin{aligned} H^{k+1}_{\mathfrak{m}}(R/(\mathfrak{a} + pR)) &= \bigoplus_{r \in \mathbb{Z}} H^k(E_p \times \mathbb{P}^n_{\mathbb{Z}/p}, \mathcal{O}_{E_p \times \mathbb{P}^n_{\mathbb{Z}/p}}(r)) \\ &= \bigoplus_{r \in \mathbb{Z}, i+j=k} H^i(E_p, \mathcal{O}_{E_p}(r)) \otimes H^j(\mathbb{P}^n_{\mathbb{Z}/p}, \mathcal{O}_{\mathbb{P}^n_{\mathbb{Z}/p}}(r)). \end{aligned}$$

Hence

$$H^{k+1}_{\mathfrak{m}}(R/(\mathfrak{a} + pR)) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if} \quad k = 1, \\ 0 & \text{if} \quad 2 \leq k \leq n, \end{cases}$$

and the Frobenius action on the one-dimensional vector space $H^2_{\mathfrak{m}}(R/(\mathfrak{a}+pR))$ may be identified with the Frobenius

$$H^1(E_p, \mathcal{O}_{E_p}) \otimes H^0(\mathbb{P}^n_{\mathbb{Z}/p}, \mathcal{O}_{\mathbb{P}^n_{\mathbb{Z}/p}}) \xrightarrow{F} H^1(E_p, \mathcal{O}_{E_p}) \otimes H^0(\mathbb{P}^n_{\mathbb{Z}/p}, \mathcal{O}_{\mathbb{P}^n_{\mathbb{Z}/p}}),$$

which is the zero map precisely when E_p is supersingular. Consequently every element of $H^2_{\mathfrak{m}}(R/(\mathfrak{a}+pR))$ is killed by the Frobenius (equivalently, by an iteration of the Frobenius) if and only if E_p is supersingular. The assertion now follows from Theorem 2.1. □

EXAMPLE 2.3. The cubic polynomial $x^3 + y^3 + z^3$ defines a smooth elliptic curve E_p in any characteristic $p \neq 3$. It is easily seen that E_p is supersingular for primes $p \equiv 2 \mod 3$, and is ordinary if $p \equiv 1 \mod 3$. Let $R = \mathbb{Z}[u, v, w, x, y, z]$. The defining ideal of $E \times \mathbb{P}^1$ is the ideal $\mathfrak{a}$ of R generated by

$$u^3 + v^3 + w^3,\ u^2x + v^2y + w^2z,\ ux^2 + vy^2 + wz^2,\ x^3 + y^3 + z^3,$$
$$vz - wy,\ wx - uz,\ uy - vx.$$

If $p \neq 3$ is a prime integer, then $H^4_{\mathfrak{a}}(R/pR) = 0$ if and only if $p \equiv 2 \mod 3$, and consequently

$$\operatorname{cd}(R/pR, \mathfrak{a}) = \begin{cases} 3 & \text{if} \quad p \equiv 2 \mod 3, \\ 4 & \text{if} \quad p \equiv 1 \mod 3. \end{cases}$$

As the above example shows, the cohomological dimension $\operatorname{cd}(R/pR, \mathfrak{a})$ varies with the characteristic p, so we cannot use local cohomology to complete the proof of Theorem 1.1 in arbitrary prime characteristic. We instead use étale cohomology to show that the defining ideal of *any* projective embedding of $E \times \mathbb{P}^1$ cannot be a set-theoretic complete intersection which, in particular, completes the proof of Theorem 1.1.

THEOREM 2.4. *Let E be a smooth elliptic curve. Then the defining ideal of any projective embedding of $E \times \mathbb{P}^1$ is not a set-theoretic complete intersection.*

PROOF. Consider an embedding $E \times \mathbb{P}^1 \subset \mathbb{P}^k$. Then the defining ideal $\mathfrak{a}$ has height $k-2$. We need to prove that $\operatorname{ara} \mathfrak{a} > k-2$, and for this we may replace the field K by its separable closure. Let ℓ be a prime integer different from the characteristic of K. We shall use the étale cohomology groups $H^i_{ét}(-; \mathbb{Z}/\ell\mathbb{Z})$, i.e., with coefficients in $\mathbb{Z}/\ell\mathbb{Z}$.

If $\mathfrak{a} = \operatorname{rad}(g_1, \dots, g_{k-2})$, then the complement U of $X = E \times \mathbb{P}^1$ in $\mathbb{P}^k$ can be covered by the affine open sets $U_j = D_+(g_j) \subset \mathbb{P}^k$ for $1 \leq j \leq k-2$. Each U_j is an affine smooth variety of dimension k, and so $H^i_{ét}(U_j; \mathbb{Z}/\ell\mathbb{Z}) = 0$ for all $i > k$ by [**16**, Thm. VI.7.2]. The Mayer-Vietoris principle [**16**, III.2.24] now implies that $H^{2k-2}_{ét}(U; \mathbb{Z}/\ell\mathbb{Z}) = 0$. We shall show that this leads to a contradiction.

Since $H^1_{ét}(E; \mathbb{Z}/\ell\mathbb{Z})$ is nonzero, the Künneth formula [**16**, VI.8.13] implies that $H^1_{ét}(X; \mathbb{Z}/\ell\mathbb{Z})$ is nonzero as well. Since X is proper, the first compactly supported étale cohomology of X is $H^1_{ét,c}(X; \mathbb{Z}/\ell\mathbb{Z}) = H^1_{ét}(X; \mathbb{Z}/\ell\mathbb{Z})$, [**16**, III.1.29]. By [**13**, (1.4a)] and [**16**, Cor. VI.11.2] there is a natural isomorphism between $H^i_{ét,c}(X; \mathbb{Z}/\ell\mathbb{Z})$ and the dual of $H^{2k-i}_{ét,X}(\mathbb{P}^k; \mathbb{Z}/\ell\mathbb{Z})$, so it follows that $H^{2k-1}_{ét,X}(\mathbb{P}^k; \mathbb{Z}/\ell\mathbb{Z})$ is nonzero. By [**16**, III.1.25] we have an exact sequence

$$H^i_{ét}(U; \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow H^{i+1}_{ét,X}(\mathbb{P}^k; \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow H^{i+1}_{ét}(\mathbb{P}^k; \mathbb{Z}/\ell\mathbb{Z}).$$

But $H^{2k-1}_{ét}(\mathbb{P}^5; \mathbb{Z}/\ell\mathbb{Z}) = 0$ by [**16**, VI.5.6], which gives a contradiction. □

3. The set-theoretically Cohen-Macaulay property

Given an affine variety V, it is an interesting question whether V supports a Cohen-Macaulay scheme, i.e., whether there exists a Cohen-Macaulay ring R such that V is isomorphic to $\operatorname{Spec} R_{\text{red}}$. More generally, let R be a regular local ring. We say that an ideal $\mathfrak{a} \subset R$ is *set-theoretically Cohen-Macaulay* if there exists an ideal $\mathfrak{b} \subset R$ with $\operatorname{rad} \mathfrak{b} = \operatorname{rad} \mathfrak{a}$ for which the ring $R/\mathfrak{b}$ is Cohen-Macaulay. A homogeneous ideal $\mathfrak{a}$ of a polynomial ring R is *set-theoretically Cohen-Macaulay* if $\mathfrak{a}R_{\mathfrak{m}}$ is a set-theoretically Cohen-Macaulay ideal of $R_{\mathfrak{m}}$, where $\mathfrak{m}$ is the homogeneous maximal ideal of R.

There is a well-known example of a determinantal ideal which is not a set-theoretic complete intersection, but is Cohen-Macaulay (and hence set-theoretically Cohen-Macaulay). For an integer $n \geq 2$, let $X = (x_{ij})$ be an $n \times (n+1)$ matrix of variables over a field K, and let R be the localization of the polynomial ring $K[x_{ij} : 1 \leq i \leq n, 1 \leq j \leq n+1]$ at its homogeneous maximal ideal. Let $\mathfrak{a}$ be the ideal of R generated by the $n \times n$ minors of the matrix X. If K has characteristic zero, then $H^{n+1}_{\mathfrak{a}}(R)$ is nonzero by an argument due to Hochster, [**9**, Remark 3.13], so $\operatorname{ara} \mathfrak{a} = n+1$. If K has positive characteristic it turns out that $H^{n+1}_{\mathfrak{a}}(R) = 0$, but nevertheless the ideal $\mathfrak{a}$ has arithmetic rank $n+1$, [**17, 2**]. In particular, $\mathfrak{a}$ is not a set-theoretic complete intersection though $R/\mathfrak{a}$ is Cohen-Macaulay.

We next show that for a smooth elliptic curve $E_{\mathbb{Q}} \subset \mathbb{P}^2_{\mathbb{Q}}$, the defining ideal of $E_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}} \subset \mathbb{P}^5_{\mathbb{Q}}$ is not set-theoretically Cohen-Macaulay. We begin with a lemma of Huneke, [**4**, page 599]. We include a proof here for the convenience of the reader.

Lemma 3.1 (Huneke). *Let $\mathfrak{a}$ be an ideal of a regular local ring R of characteristic $p > 0$. If the ring $R/\mathfrak{a}$ is F-pure and not Cohen-Macaulay, then the ideal $\mathfrak{a}$ is not set-theoretically Cohen-Macaulay.*

Proof. Note that $\mathfrak{a}$ is a radical ideal since $R/\mathfrak{a}$ is F-pure. Let $\mathfrak{b}$ be an ideal of R with $\operatorname{rad} \mathfrak{b} = \mathfrak{a}$, and choose $x_1, \dots, x_d \in R$ such that their images form a system of parameters for $R/\mathfrak{a}$ and $R/\mathfrak{b}$. Since $R/\mathfrak{a}$ is is not Cohen-Macaulay, there exist $k \in \mathbb{N}$ and $y \in R$ such that

$$yx_k \in (x_1, \dots, x_{k-1})R + \mathfrak{a} \quad \text{and} \quad y \notin (x_1, \dots, x_{k-1})R + \mathfrak{a}.$$

Let $q = p^e$ be a prime power such that $\mathfrak{a}^{[q]} \subseteq \mathfrak{b}$. Then

$$y^q x_k^q \in (x_1^q, \dots, x_{k-1}^q)R + \mathfrak{a}^{[q]} \ \subseteq\ (x_1^q, \dots, x_{k-1}^q)R + \mathfrak{b}.$$

If $R/\mathfrak{b}$ is Cohen-Macaulay, then

$$y^q \in (x_1^q, \dots, x_{k-1}^q)R + \mathfrak{b} \ \subseteq\ (x_1^q, \dots, x_{k-1}^q)R + \mathfrak{a}.$$

The hypothesis that $R/\mathfrak{a}$ is F-pure implies that $y \in (x_1, \dots, x_{k-1})R + \mathfrak{a}$, which is a contradiction. $\square$

For the remainder of this section, $R_{\mathbb{Z}}$ will denote a polynomial ring over the integers, and we use the notation $R_{\mathbb{Q}} = R_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $R_p = R_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$.

Lemma 3.2. *Let $\mathfrak{a}$ be an ideal of $R_{\mathbb{Z}} = \mathbb{Z}[z_1, \dots, z_m]$, and consider the multiplicative set $W = R_{\mathbb{Z}} \setminus (z_1, \dots, z_m)R_{\mathbb{Z}}$. If $W^{-1}R_{\mathbb{Q}}/\mathfrak{a}W^{-1}R_{\mathbb{Q}}$ is Cohen-Macaulay, then the rings $W^{-1}R_p/\mathfrak{a}W^{-1}R_p$ are Cohen-Macaulay for all but finitely many prime integers p.*

Proof. Let $x_1, \dots, x_d \in R_{\mathbb{Z}}$ be elements whose images form a system of parameters for $W^{-1}R_{\mathbb{Q}}/\mathfrak{a}W^{-1}R_{\mathbb{Q}}$. Since this ring is Cohen-Macaulay, there exists an element f in the multiplicative set W such that $x_1, \dots, x_d$ is a regular sequence on $S/\mathfrak{a}S$ where $S = R_{\mathbb{Z}}[f^{-1}]$. Moreover, we may choose f in such a way that

$$z_i \in \operatorname{rad}(\mathfrak{a}S + (x_1, \dots, x_d)S), \qquad 1 \le i \le m.$$

These conditions are preserved if we enlarge the ring S by inverting finitely many nonzero integers. By the result on generic freeness, [**15**, Theorem 24.1], we may assume (after replacing f by a nonzero integer multiple uf and S by its localization at the element u) that S, $S/\mathfrak{a}$, and each of

$$\frac{S}{\mathfrak{a}S + (x_1, \dots, x_i)S}, \qquad 1 \le i \le d,$$

are free $\mathbb{Z}[u^{-1}]$-modules. In particular, for all $1 \le i \le d-1$, we have short exact sequences of free $\mathbb{Z}[u^{-1}]$-modules,

$$0 \longrightarrow \frac{S}{\mathfrak{a}S+(x_1,\dots,x_i)S} \xrightarrow{\ x_{i+1}\ } \frac{S}{\mathfrak{a}S+(x_1,\dots,x_i)S} \longrightarrow \frac{S}{\mathfrak{a}S+(x_1,\dots,x_{i+1})S} \longrightarrow 0.$$

Let p be any prime integer not dividing u, and apply $(-) \otimes_{\mathbb{Z}[u^{-1}]} \mathbb{Z}/p\mathbb{Z}$ to the sequences above. The resulting exact sequences show that $x_1, \dots, x_d$ is a regular sequence on

$$\frac{S}{\mathfrak{a}S} \otimes_{\mathbb{Z}[u^{-1}]} \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \frac{R_p[f^{-1}]}{\mathfrak{a}R_p[f^{-1}]},$$

and hence on $W^{-1}R_p/\mathfrak{a}W^{-1}R_p$ as required. □

THEOREM 3.3. *Let $E_{\mathbb{Q}} \subset \mathbb{P}^2_{\mathbb{Q}}$ be a smooth elliptic curve. Then the defining ideal of the Segre embedding $E_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}} \subset \mathbb{P}^5_{\mathbb{Q}}$ is not set-theoretically Cohen-Macaulay.*

PROOF. Let $\mathfrak{a} \subset R_{\mathbb{Z}} = \mathbb{Z}[z_{ij} : 0 \le i \le 2,\ 0 \le j \le 1]$ be an ideal such that $\mathfrak{a}R_{\mathbb{Q}} \subset R_{\mathbb{Q}}$ is the defining ideal of $E_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}} \subset \mathbb{P}^5_{\mathbb{Q}}$. There exist infinitely many prime integers p such that $E_p \subset \mathbb{P}^2_{\mathbb{Z}/p}$ is a smooth ordinary elliptic curve. For these infinitely many primes, the ring $R_p/\mathfrak{a}R_p$ is F-pure and not Cohen-Macaulay, and hence the ideal $\mathfrak{a}R_p$ is not set-theoretically Cohen-Macaulay by Lemma 3.1. It now follows from Lemma 3.2 that the ideal $\mathfrak{a}R_{\mathbb{Q}} \subset R_{\mathbb{Q}}$ is not set-theoretically Cohen-Macaulay. □

REMARK 3.4. If $E_p \subset \mathbb{P}^2_{\mathbb{Z}/p}$ is an ordinary elliptic curve, then the defining ideal of the Segre embedding $E_p \times \mathbb{P}^1_{\mathbb{Z}/p} \subset \mathbb{P}^5_{\mathbb{Z}/p}$ is not set-theoretically Cohen-Macaulay by Lemma 3.1, since the corresponding homogeneous coordinate ring is F-pure and not Cohen-Macaulay. If E is supersingular, we do not know whether the defining ideal is set-theoretically Cohen-Macaulay.

REMARK 3.5. Lemma 3.1 can be strengthened by Lyubeznik's theorem as follows: Let $(R, \mathfrak{m})$ be a regular local ring of positive characteristic, and $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of R such that $R/\mathfrak{a}$ is F-pure and $\operatorname{rad}\mathfrak{b} = \mathfrak{a}$. If the local cohomology module $H^i_{\mathfrak{m}}(R/\mathfrak{a})$ is nonzero for some integer i, then Theorem 2.1 implies that

$$H^{\dim R - i}_{\mathfrak{a}}(R) = H^{\dim R - i}_{\mathfrak{b}}(R)$$

is nonzero as well. Using Theorem 2.1 once again, it follows that $H^i_{\mathfrak{m}}(R/\mathfrak{b})$ is nonzero. This implies in particular that

$$\operatorname{depth} R/\mathfrak{a} \ge \operatorname{depth} R/\mathfrak{b}.$$

Consequently if $\mathfrak{b}$ is an ideal of a regular local ring R of positive characteristic such that $R/\operatorname{rad}\mathfrak{b}$ is F-pure, then

$$\operatorname{depth} R/\operatorname{rad}\mathfrak{b} \ge \operatorname{depth} R/\mathfrak{b}.$$

This is false without the assumption that $R/\operatorname{rad}\mathfrak{b}$ is F-pure: let $R = K[[w, x, y, z]]$ where K is a field of positive characteristic, and consider the ideal

$$\mathfrak{p} = (xy - wz, y^3 - xz^2, wy^2 - x^2z, x^3 - w^2y) \subset R.$$

Then $R/\mathfrak{p} \cong K[[s^4, s^3t, st^3, t^4]]$ which is not Cohen-Macaulay. Hartshorne proved that $\mathfrak{p}$ is a set-theoretic complete intersection, i.e., that $\mathfrak{p} = \operatorname{rad}(f, g)$ for elements $f, g \in R$, [**6**]. Hence, in this example,

$$\operatorname{depth} R/\operatorname{rad}(f, g) = 1 < \operatorname{depth} R/(f, g) = 2.$$

Acknowledgments

It is a pleasure to thank Gennady Lyubeznik for several helpful discussions.

References

[1] R. Bott and L. W. Tu, *Differential forms in algebraic topology*, Graduate Texts in Mathematics, vol. 82, Springer-Verlag, New York, 1982.
[2] W. Bruns and R. Schwänzl, *The number of equations defining a determinantal variety*, Bull. London Math. Soc. **22** (1990), no. 5, 439–445.
[3] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
[4] D. Eisenbud, M. Mustaţă, and M. Stillman, *Cohomology on toric varieties and local cohomology with monomial supports*, J. Symbolic Comput. **29** (2000), no. 4-5, 583–600, Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998).
[5] N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbf{Q}$, Invent. Math. **89** (1987), no. 3, 561–567.
[6] R. Hartshorne, *Complete intersections in characteristic* $p > 0$, Amer. J. Math. **101** (1979), no. 2, 380–383.
[7] R. Hartshorne and R. Speiser, *Local cohomological dimension in characteristic* p, Ann. of Math. (2) **105** (1977), no. 1, 45–79.
[8] M. Hochster and J. L. Roberts, *The purity of the Frobenius and local cohomology*, Advances in Math. **21** (1976), no. 2, 117–172.
[9] C. Huneke and G. Lyubeznik, *On the vanishing of local cohomology modules*, Invent. Math. **102** (1990), no. 1, 73–93.
[10] B. Iversen, *Cohomology of sheaves*, Universitext, Springer-Verlag, Berlin, 1986.
[11] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Springer-Verlag, Berlin, 1976, Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504.
[12] G. Lyubeznik, *The number of defining equations of affine algebraic sets*, Amer. J. Math. **114** (1992), no. 2, 413–463.
[13] ———, *Étale cohomological dimension and the topology of algebraic varieties*, Ann. of Math. (2) **137** (1993), no. 1, 71–128.
[14] ———, *On the vanishing of local cohomology in characteristic* $p > 0$, Preprint (2004).
[15] H. Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989.
[16] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
[17] P. E. Newstead, *Some subvarieties of Grassmannians of codimension* 3, Bull. London Math. Soc. **12** (1980), no. 3, 176–182.

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332.
E-mail address: singh@math.gatech.edu

Department of Mathematics, Purdue University, West Lafayette, IN 47907.
E-mail address: walther@math.purdue.edu