ON 2-SUPERIRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

J. W. BOBER, L. DU, D. FRETWELL, G. S. KOPP, AND T. D. WOOLEY

ABSTRACT. We investigate k-superirreducible polynomials, by which we mean irreducible polynomials that remain irreducible under any polynomial substitution of positive degree at most k. Let $\mathbb{F}$ be a finite field of characteristic p. We show that no 2-superirreducible polynomials exist in $\mathbb{F}[t]$ when $p = 2$ and that no such polynomials of odd degree exist when p is odd. We address the remaining case in which p is odd and the polynomials have even degree by giving an explicit formula for the number of monic 2-superirreducible polynomials having even degree d. This formula is analogous to that given by Gauss for the number of monic irreducible polynomials of given degree over a finite field. We discuss the associated asymptotic behaviour when either the degree of the polynomial or the size of the finite field tends to infinity.

1. INTRODUCTION

Superirreducible polynomials are polynomials that resist factorization under polynomial substitutions. Let R be a commutative domain with unity having field of fractions F, and consider a polynomial $f \in R[t]$. For each natural number k, we say that f is *weakly k-superirreducible* over R if $f(g(t))$ is irreducible over $F[t]$ for all polynomials $g \in R[t]$ having degree k. If the polynomial f is weakly k-superirreducible over R for $1 \leq k \leq K$, then we say that f is *K-superirreducible*. In this hierarchy, a 1-superirreducible polynomial is simply an irreducible polynomial. It transpires that a polynomial may be weakly k-superirreducible and yet not weakly $(k-1)$-superirreducible (and consequently, not k-superirreducible). For example, one may check that $x^6+x^5+x^3+x^2+1$ is weakly 3-superirreducible over $\mathbb{F}_2$ yet not weakly 2-superirreducible. When $d \geq 2$ and $f \in R[t]$ has degree d, a consideration of the polynomial $f(t+f(t))$ reveals that f cannot be k-superirreducible whenever $k \geq d$. The situation when $2 \leq k < d$ is more subtle, however, and our focus in this paper lies on the simplest situation here in which $k = 2$ and R is a finite field. Let $\mathbb{F}_q$ denote the finite field of q elements, and when $1 \leq k < d$, denote by $s_k(q,d)$ the number of monic weakly k-superirreducible polynomials lying in $\mathbb{F}_q[t]$ having degree d. In Proposition 3.6, we provide an explicit formula for $s_2(q,d)$ analogous to the formula given by Gauss for the number of monic irreducible polynomials of given degree over $\mathbb{F}_q$. A consequence of this formula delivers the asymptotic formula recorded in our first theorem.

Theorem 1.1. *For q a prime power and d a positive integer, the number of 2-superirreducible polynomials of degree d satisfies:*

(a) $s_2(q,d) = 0$ *whenever either q is a power of 2 or d is odd;*
(b) $s_2(q,d) = 0$ *whenever $q > (d-1)^2$;*
(c) *when q is odd and $d \to \infty$ through the even integers,*

$$s_2(q,d) = \frac{q^d}{d2^q} + O\left(\frac{1}{d}q^{d/2}\right). \tag{1.1}$$

1991 *Mathematics Subject Classification.* 11T06, 12E05, 11S05.

Key words and phrases. Irreducibility, finite fields, polynomial compositions.

Superirreducibility has in fact been studied in the past, although not by name. Strengthening the above pedestrian observation concerning $f(t+f(t))$, it follows from work of Schinzel [8, Lemma 10] that a polynomial of degree $d \geq 3$ lying in $\mathbb{Q}[t]$ cannot be $(d-1)$-superirreducible. More recently, Bober et al. [2] have considered superirreducibility as a potential limitation to the understanding of smooth integral values of polynomials. More precisely, these authors show in [2, Theorem 1.1] that quadratic polynomials $f \in \mathbb{Q}[t]$ admit polynomial substitutions $g \in \mathbb{Q}[t]$ of arbitrarily high degree k having the property that all of the factors of $f(g(t))$ have degree $O(k/\sqrt{\log\log k})$. Consider a positive number ε and an integer k sufficiently large in terms of ε. Then on taking m to be an integer large enough in terms of both ε and k, it follows that with $n = g(m)$, the polynomial value $f(n)$ has all of its prime factors smaller than n^{ε} (see [2, Corollary 1.2]). This provides strong information about smooth values $f(n)$ for $n \in \mathbb{Z}$. It is thus important to understand polynomials f (in degree higher than 2) that resist such factorizations of compositions $f(g(t))$, since the existence of smooth values of such polynomials will necessarily be particularly challenging to establish. In [2, Section 6], it is shown that 2-superirreducible polynomials exist in $\mathbb{Q}[t]$ having degree 6. Moreover, in work contemporaneous with that reported on herein, the thesis of Du [3, Theorem 1.9.1] has exhibited some infinite families of 2-superirreducible polynomials in $\mathbb{Q}[t]$ of degree 4, including the simple examples $f(t) = t^4 + 1$ and $f(t) = t^4 + 2$.

With a potential local-global principle in mind, it might be expected that insights into the superirreducibility of polynomials over $\mathbb{Z}$ and over $\mathbb{Q}$ might be gained by examining corresponding superirreducibility properties over the p-adic integers $\mathbb{Z}_p$ and p-adic numbers $\mathbb{Q}_p$. Such considerations lead in turn to an investigation of the superirreducibility of polynomials over finite fields. We finish our paper by disappointing the reader in Section 4 with the news that if $k \geq 2$ and p is any prime number, then k-superirreducible polynomials exist over neither $\mathbb{Z}_p$ nor $\mathbb{Q}_p$.

Other authors have considered arithmetic properties of compositions, especially compositional iterates, of polynomials within the context of arithmetic dynamics. See the papers [6, 7] and the survey [1, Section 19] for a wide variety of results and questions concerning irreducibility of polynomial iterates and composites.

2. Basic lemmas

In this section we prove the basic lemmas that provide the infrastructure for our subsequent discussions concerning superirreducibility. Recall the definition of k-superirreducibility provided in our opening paragraph. We begin by expanding on the observation that there are no weakly k-superirreducible polynomials of degree k or larger.

Lemma 2.1. *Let R be a commutative domain with unity, and let $f \in R[t]$ be a polynomial of degree $d \geq 2$. Then $f(t)$ is not weakly k-superirreducible for any $k \geq d$.*

Proof. For each non-negative integer r, consider the degree $d+r$ substitution $g(t) = t + t^r f(t)$. We have

$$f(g(t)) = f(t + t^r f(t)) \equiv f(t) \equiv 0 \pmod{f(t)}.$$

Thus, we see that $f(g(t))$ is divisible by $f(t)$, and it is hence reducible. It follows that f is not weakly k-superirreducible for $k \geq d$. □

The next lemma is a mild generalization of [2, Proposition 3.1] to arbitrary fields. The latter proposition is restricted to the rational field $\mathbb{Q}$, and we would be remiss were we not to record that Schinzel [9, Theorem 22] attributes this conclusion to Capelli.

Lemma 2.2. *Let K be a field. Suppose that $f(x) \in K[x]$ is a monic irreducible polynomial, let α be a root of f lying in a splitting field extension for f over K, and put $L = K(\alpha)$. Then, for any non-constant polynomial $g(t) \in K[t]$, the polynomial $f(g(t))$ is reducible in $K[t]$ if and only if $g(t) - \alpha$ is reducible in $L[t]$.*

Proof. We consider the K-algebra $A = K[x,t]/(f(x), g(t) - x)$ from two perspectives. First, on noting that $f(x)$ is irreducible over $K[x]$, we find that $K[x]/(f(x)) \cong K[\alpha] = K(\alpha) = L$. Thus, on the one hand,

$$A \cong \frac{K[x,t]/(f(x))}{(g(t) - x)} \cong L[t]/(g(t) - \alpha).$$

Here, of course, we view $(g(t)-x)$ as being an ideal in $K[x,t]/(f(x))$. On the other hand, similarly,

$$A \cong \frac{K[x,t]/(g(t) - x)}{(f(x))} \cong K[t]/(f(g(t))).$$

Thus, we obtain a K-algebra isomorphism

$$K[t]/(f(g(t))) \cong L[t]/(g(t) - \alpha). \tag{2.1}$$

Hence $K[t]/(f(g(t)))$ is a field if and only if $L[t]/(g(t)-\alpha)$ is a field, and thus $f(g(t))$ is irreducible in $K[t]$ if and only if $g(t) - \alpha$ is irreducible in $L[t]$. The desired conclusion follows. □

We take the opportunity to record a further consequence of the relation (2.1), since it may be of use in future investigations concerning superirreducibility.

Lemma 2.3. *Let K be a field. Suppose that $f(x) \in K[x]$ is a monic irreducible polynomial, and let $g(t) \in K[t]$ be any non-constant polynomial. Then, for any polynomial divisor $h(t)$ of $f(g(t))$, we have* $\deg(f) | \deg(h)$.

Proof. The relation (2.1) shows that $K[t]/(f(g(t))$ has the structure of an L-algebra. Any ring quotient of an L-algebra is still an L-algebra. Thus, we see that $K[t]/(h(t))$ is an L-algebra, and in particular a vector space over L. Consequently, one has

$$\deg(h) = \dim_K K[t]/(h(t)) = [L : K]\left(\dim_L K[t]/(h(t))\right) = \deg(f)\left(\dim_L K[t]/(h(t))\right),$$

and thus $\deg(f) | \deg(h)$. □

We also provide a trivial lemma explaining the relationship between our definitions of superirreducibility and weak superirreducibility for different values of k.

Lemma 2.4. *Let R be a commutative domain with unity, and let $f(x) \in R[x]$ and $k \in \mathbb{N}$. The polynomial $f(x)$ is k-superirreducible if and only if it is weakly ℓ-superirreducible for all natural numbers $\ell \leq k$. The polynomial $f(x)$ is weakly k-superirredcubible if and only if it is weakly ℓ-superirreducible for all natural numbers ℓ dividing k.*

Proof. All of the implications follow formally from the definitions except for the statement that, if $f(x)$ is weakly k-superirreducible and $\ell | k$, then $f(x)$ is weakly ℓ-superirreducible. To prove this, write $k = \ell m$ and consider a polynomial $g(t)$ of degree ℓ. The substitution $f(g(t^m))$ is thus irreducible, and hence so is $f(g(t))$. □

It follows that "2-superirreducible" and "weakly 2-superirreducible" are synonyms.

3. Counting 2-superirreducible polynomials over finite fields

Recall that when $1 \le k < d$, we write $s_k(q,d)$ for the number of monic weakly k-superirreducible polynomials lying in $\mathbb{F}_q[t]$ having degree d. In particular, the concluding remark of the previous section shows that $s_2(q,d)$ is the number of monic 2-superirreducible polynomials in $\mathbb{F}_q[t]$ having degree d. Our goal in this section is to establish formulae for $s_2(q,d)$ that deliver the conclusions recorded in Theorem 1.1.

3.1. **Elementary cases.**

We begin by confirming that when q is a power of 2, and also when d is odd, one has $s_2(q,d)=0$. In fact, rather more is true, as we now demonstrate.

Proposition 3.1. *Let p be a prime. Then for all natural numbers ℓ and d, one has $s_p(p^\ell,d)=0$.*

Proof. Consider a polynomial $f \in \mathbb{F}_{p^\ell}[t]$ having degree d. Write $f(x)=\sum_{j=0}^d a_j x^j$, and note that $a_j = a_j^{p^\ell}$ for each index j. Thus, we have

$$f(t^p)=\sum_{j=0}^d a_j^{p^\ell} t^{pj} = \left(\sum_{j=0}^d a_j^{p^{\ell-1}} t^j \right)^p,$$

and it follows that $f(x)$ is not weakly p-superirreducible. Consequently, one has $s_p(p^\ell,d)=0$. □

The special case $p=2$ of Proposition 3.1 shows that $s_2(q,d)=0$ when q is a power of 2. Next, we turn to polynomials of odd degree over $\mathbb{F}_q$.

Proposition 3.2. *When d is an odd natural number, one has $s_2(q,d)=0$.*

Proof. In view of the case $p=2$ of Proposition 3.1, there is no loss of generality in assuming that q is odd. Let $f(x)\in\mathbb{F}_q[x]$ be a monic irreducible polynomial of degree d. The polynomial f has a root α lying in $\mathbb{F}_{q^d}$, and $\mathbb{F}_{q^d}=\mathbb{F}_q(\alpha)$. By virtue of Lemma 2.2, if we are able to find a quadratic polynomial $g(t)\in\mathbb{F}_q[t]$ having the property that $g(t)-\alpha$ has a root in $\mathbb{F}_{q^d}$, then we may infer that $f(g(t))$ is reducible. This will confirm that $f(x)$ is not 2-superirreducible, delivering the desired conclusion.

We may divide into two cases:

(a) Suppose first that $\alpha=\beta^2$ for some $\beta\in\mathbb{F}_{q^d}$. Then we put $g(t)=t^2$ and observe that the polynomial $g(t)-\alpha$ has the root $\beta\in\mathbb{F}_{q^d}$.

(b) In the remaining cases, we may suppose that α is not the square of any element of $\mathbb{F}_{q^d}$. Since $q\ne 2$, there exists an element $b\in\mathbb{F}_q$ which is not the square of any element of $\mathbb{F}_q$. On recalling our assumption that d is odd, we find that b is not the square of any element in $\mathbb{F}_{q^d}$. Thus, we may infer that $b^{-1}\alpha=\beta^2$ for some $\beta\in\mathbb{F}_{q^d}$. We now put $g(t)=bt^2$ and observe that the polynomial $g(t)-\alpha$ has the root $\beta\in\mathbb{F}_{q^d}$.

In either case, our previous discussion shows that $f(x)$ is not 2-superirreducible, and this implies the desired conclusion. □

The conclusion of Proposition 3.2 combines with that of Proposition 3.1 to confirm the first assertion of Theorem 1.1. These cases of Theorem 1.1 help to explain the example noted in the introduction demonstrating that weak $(k-1)$-superirreducibility is not necessarily inherited from the corresponding property of weak k-superirreducibility. Expanding a little on that example, we observe that by making use of commonly available computer algebra packages, one finds the following examples of polynomials weakly 3-superirreducible over $\mathbb{F}_2[x]$ yet not 2-superirreducible over $\mathbb{F}_2[x]$:

$$\begin{aligned} x^6+x^5+x^3+x^2 &+1,\\ x^8+x^6+x^5+x^3 &+1,\\ x^{10}+x^9+x^7+x^2 &+1,\\ x^{10}+x^9+x^8+x^4+x^3+x^2 &+1,\\ x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x^2 &+1. \end{aligned}$$

In each of these examples of a polynomial $f \in \mathbb{F}_2[x]$, the failure of 2-superirreducibility follows from Proposition 3.1. Meanwhile, a direct computation confirms that the polynomial $f(g(t))$ is irreducible over $\mathbb{F}_2[t]$ for each of the 8 possible monic cubic polynomials $g(t)$ lying in $\mathbb{F}_2[t]$. No analogous odd degree examples are available, of course, by virtue of Proposition 3.2, though examples of larger even degrees are not too difficult to identify.

3.2. **Heuristics.** We next address the problem of determining a formula for the number $s_k(q,d)$ of monic weakly k-superirreducible polynomials of degree d over $\mathbb{F}_q$. The simplest situation here with $k=1$ is completely resolved by celebrated work of Gauss, since 1-superirreducibility is equivalent to irreducibility. Thus, as is well-known, it follows from Gauss [4, p. 602] that

$$s_1(q,d)=\frac{1}{d}\sum_{e|d}\mu\left(\frac{d}{e}\right)q^e,$$

whence, as $d\to\infty$, one has the asymptotic formula

$$s_1(q,d)=\frac{q^d}{d}+O\left(\frac{1}{d}q^{d/2}\right).$$

The corresponding situation with $k\geq 2$ is more subtle. We now motivate our proof of an asymptotic formula for $s_2(q,d)$ with a heuristic argument that addresses the cases remaining to be considered, namely those where d is even and q is odd. The heuristic argument is based on the following lemma, which will also be used in the proof.

Lemma 3.3. *Let q be an odd prime power, and let $f(x)\in\mathbb{F}_q[x]$ be a monic irreducible polynomial of even degree d. Let $\alpha\in\mathbb{F}_{q^d}$ be a root of $f(x)$. The polynomial $f(x)$ is 2-superirreducible if and only if $\alpha+c$ is not a square in $\mathbb{F}_{q^d}$ for all $c\in\mathbb{F}_q$.*

Proof. As a consequence of Lemma 2.2, the polynomial $f(x)$ is 2-superirreducible in $\mathbb{F}_q[x]$ if and only if $g(t)-\alpha$ is irreducible in $\mathbb{F}_{q^d}[t]$ for all quadratic polynomials $g\in\mathbb{F}_q[t]$. Since this condition is invariant under all additive shifts mapping t to $t+v$, for $v\in\mathbb{F}_q$, it suffices to consider only the quadratic polynomials of the shape $g(t)=at^2-b$, with $a,b\in\mathbb{F}_q$. Moreover, the assumption that d is even ensures that a is a square in $\mathbb{F}_{q^d}$, and hence we may restrict our attention further to polynomials of the shape $g(t)=t^2-c$ with $c\in\mathbb{F}_q$. So $f(x)$ is 2-superirreducible if and only if the equation $t^2-c=\alpha$ has no solution in $\mathbb{F}_{q^d}$ for any $c\in\mathbb{F}_q$. □

For heuristic purposes, we now model the behaviour of these elements $\alpha+c$ as if they are randomly distributed throughout $\mathbb{F}_{q^d}$. Since roughly half the elements of $\mathbb{F}_{q^d}$ are squares, one should expect that the condition that $\alpha+c$ is not a square is satisfied for a fixed choice of c with probability close to $\frac{1}{2}$. Treating the conditions for varying $c\in\mathbb{F}_q$ as independent events, we therefore expect that $f(x)$ is 2-superirreducible with probability close to $1/2^q$. Multiplying this probability by the number of choices for monic irreducible polynomials $f(x)$ of degree d, our heuristic predicts that when d is even and q is odd, one should have

$$s_2(q,d) \approx \frac{q^d}{d2^q}.$$

We shall see in the next subsection that this heuristic accurately predicts the asymptotic behaviour of $s_2(q,d)$ as $d \to \infty$ through even integers d.

3.3. **The large d limit.** The asymptotic formula predicted by the heuristic described in the previous subsection will follow in the large d limit from Weil's resolution of the Riemann hypothesis for curves over finite fields. We make use, specifically, of the Weil bound for certain higher autocorrelations of the quadratic character generalizing Jacobi sums. Our goal in this subsection is the proof of the estimate for $s_2(q,d)$ supplied by the following theorem, an immediate consequence of which is the asymptotic formula (1.1) supplied by Theorem 1.1.

Theorem 3.4. *When q is odd and d is even, one has*

$$\left| s_2(q,d) - \frac{q^d}{d2^q} \right| < \frac{q}{2d} q^{d/2}.$$

The proof of this estimate is based on a more rigorous version of the heuristic argument given in Section 3.2, and it employs character sums that we now define.

Definition 3.5. Let q be an odd prime power, and write χ_q for the nontrivial quadratic character $\chi_q : \mathbb{F}_q^\times \to \{1,-1\}$, extended to $\mathbb{F}_q$ by setting $\chi_q(0) = 0$. We define the *order n autocorrelation of* χ_q with offsets $u_1, \dots, u_n \in \mathbb{F}_q$ to be the sum

$$a_q(u_1,\dots,u_n) = \sum_{\beta \in \mathbb{F}_q} \chi_q(\beta + u_1) \cdots \chi_q(\beta + u_n).$$

Noting that this definition is independent of the ordering of the arguments, when $U = \{u_1, \dots, u_n\}$ is a subset of $\mathbb{F}_q$, we adopt the convention of writing $a_q(U)$ for $a_q(u_1,\dots,u_n)$.

Note that $a_q(U) \in \mathbb{Z}$ for all subsets U of $\mathbb{F}_q$. When $|U| = 1$ it is apparent that $a_q(U) = 0$. Meanwhile, in circumstances where $|U| = 2$, so that $U = \{u_1, u_2\}$ for some elements $u_1, u_2 \in \mathbb{F}_q$ with $u_1 \neq u_2$, the autocorrelation $a_q(U) = a_q(u_1,u_2)$ is a quadratic Jacobi sum. Thus, in this situation, we have $a_q(u_1,u_2) = \pm 1$; see [5, Chapter 8]. The higher-order correlations become more complicated, but we will see that they can easily be bounded. First, we relate the autocorrelations of χ_q to the number $s_2(q,d)$ of monic 2-superirreducible polynomials of degree d in $\mathbb{F}_q[x]$.

Proposition 3.6. *Let q be an odd prime power and d be even. Then*

$$s_2(q,d) = \frac{1}{d2^q} \sum_{\substack{e \mid d \\ d/e \text{ odd}}} \mu\Big(\frac{d}{e}\Big) \bigg(q^e + \sum_{\emptyset \neq U \subseteq \mathbb{F}_q} (-1)^{|U|} a_{q^e}(U) \bigg).$$

Proof. Consider a monic irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d, and let α be a root of $f(x)$ in $\mathbb{F}_{q^d}$. It follows from Lemma 3.3 that $f(x)$ is 2-superirreducible if and only if $\alpha + c$ is not a square in $\mathbb{F}_{q^d}$ for each $c \in \mathbb{F}_q$. Since the latter condition is equivalent to the requirement that $\chi_{q^d}(\alpha + c) = -1$ for all $c \in \mathbb{F}_q$, we see that

$$\prod_{c \in \mathbb{F}_q} \frac{1}{2}\left(1 - \chi_{q^d}(\alpha + c)\right) = \begin{cases} 1, & \text{if } f \text{ is 2-superirreducible,} \\ 0, & \text{otherwise.} \end{cases}$$

This relation provides an algebraic formulation of the indicator function for 2-superirreducibility. Instead of summing this quantity over monic irreducible polynomials, we can instead sum over elements $\alpha \in \mathbb{F}_{q^d}$ not lying in any proper subfield, dividing by d to account for overcounting. Thus, we find that

$$s_2(q,d) = \frac{1}{d} \sum_{\substack{\alpha \in \mathbb{F}_{q^d} \\ \alpha \notin \mathbb{F}_{q^e}\ (e<d \text{ and } e|d)}} \prod_{c \in \mathbb{F}_q} \frac{1}{2} \left(1 - \chi_{q^d}(\alpha + c)\right).$$

The condition on α in the first summation of this relation may be encoded using the Möbius function. Thus, we obtain

$$s_2(q,d) = \frac{1}{d2^q} \sum_{e|d} \mu\Big(\frac{d}{e}\Big) \sum_{\alpha \in \mathbb{F}_{q^e}} \prod_{c \in \mathbb{F}_q} \left(1 - \chi_{q^d}(\alpha + c)\right).$$

When d/e is even, the quadratic character χ_{q^d} on $\mathbb{F}_{q^d}$ restricts to the trivial character on $\mathbb{F}_{q^e}$, and when d/e is odd, it instead restricts to χ_{q^e}. We therefore deduce that

$$s_2(q,d) = \frac{1}{d2^q} \sum_{\substack{e|d \\ d/e \text{ odd}}} \mu\Big(\frac{d}{e}\Big) \sum_{\alpha \in \mathbb{F}_{q^e}} \prod_{c \in \mathbb{F}_q} \left(1 - \chi_{q^e}(\alpha + c)\right),$$

and on observing that

$$\sum_{\alpha \in \mathbb{F}_{q^e}} \prod_{c \in \mathbb{F}_q} \left(1 - \chi_{q^e}(\alpha + c)\right) = q^e + \sum_{\emptyset \neq U \subseteq \mathbb{F}_q} (-1)^{|U|} a_{q^e}(U),$$

the desired formula for $s_2(q,d)$ follows. □

We next establish a bound on the autocorrelations $a_{q^e}(U)$.

Lemma 3.7. *Let q be an odd prime power. Suppose that U is a non-empty subset of $\mathbb{F}_q$ with $|U| = n$. Then for each positive integer e, one has $|a_{q^e}(U)| \leq (n-1)q^{e/2}$.*

Proof. Observe that

$$a_{q^e}(U) = \sum_{\beta \in \mathbb{F}_{q^e}} \chi_{q^e}(h(\beta)),$$

where $h(t) = (t+u_1)\cdots(t+u_n)$ is a polynomial in $\mathbb{F}_q[t]$ having roots $-u_1, \ldots, -u_n$. Since $u_1, \ldots, u_n$ are distinct and χ_{q^e} is a multiplicative character of order 2, it follows from a version of Weil's bound established by Schmidt that $|a_{q^e}(U)| \leq (n-1)q^{e/2}$; see [10, Chapter 2, p. 43, Theorem 2C']. □

Now we complete the proof of Theorem 3.4. In this proof, we expend a little extra effort to achieve a more attractive conclusion.

Proof of Theorem 3.4. We begin by observing that, in view of Lemma 3.7, one has

$$\begin{aligned} \Big| \sum_{\emptyset \neq U \subseteq \mathbb{F}_q} (-1)^{|U|} a_{q^e}(U) \Big| &\leq \sum_{n=1}^{q} \binom{q}{n} (n-1) q^{e/2} \\ &= q^{e/2} \Bigg(q \sum_{n=2}^{q} \binom{q-1}{n-1} - \sum_{n=2}^{q} \binom{q}{n} \Bigg) \\ &= q^{e/2} \big(q(2^{q-1} - 1) - (2^q - q - 1) \big). \end{aligned} \tag{3.1}$$

We note next that since d is assumed to be even, then whenever e is a divisor of d with d/e odd, it follows that e is even. Moreover, if it is the case that $e < d$, then $e \leq d/3$. The first constraint on e here conveys us from (3.1) to the upper bound

$$\sum_{\substack{e|d\\ d/e \text{ odd}}} \left| \sum_{\emptyset \neq U \subseteq \mathbb{F}_q} (-1)^{|U|} a_{q^e}(U) \right| \leq \left(2^{q-1}(q-2)+1\right) \sum_{m=0}^{d/2} q^m$$

$$< \frac{q}{q-1}\left(2^{q-1}(q-2)+1\right) q^{d/2}.$$

Meanwhile, making use also of the second constraint on e, we obtain the bound

$$\sum_{\substack{e|d\\ e<d \text{ and } d/e \text{ odd}}} q^e \leq \sum_{0 \leq m \leq d/3} q^m < \frac{q}{q-1} q^{d/2}.$$

By applying these bounds in combination with Proposition 3.6, we deduce that

$$\left| s_2(q,d) - \frac{q^d}{d2^q} \right| < \frac{1}{d2^q}\left((q-1)2^{q-1} - 2^{q-1} + 2\right) \frac{q}{q-1} q^{d/2} \leq \frac{q}{2d} q^{d/2}.$$

This completes the proof of Theorem 3.4. □

3.4. **Vanishing in the large q limit.** We turn our attention next to the behaviour of $s_2(q,d)$ when d is fixed and q is large. It transpires that $s_2(q,d) = 0$ for large enough prime powers q. This conclusion follows from Lemma 3.3 once we confirm that for every primitive element $\alpha \in \mathbb{F}_{q^d}$, there exists an element $c \in \mathbb{F}_q$ for which $\chi_{q^d}(\alpha + c) = 1$.

Lemma 3.8. *Suppose that q is an odd prime power and $\alpha \in \mathbb{F}_{q^d}$ is a primitive element. Then, whenever $q > (d-1)^2$, one has*

$$\left| \sum_{c \in \mathbb{F}_q} \chi_{q^d}(\alpha + c) \right| < q.$$

Proof. Consider the d-dimensional commutative $\mathbb{F}_q$-algebra $\mathbb{F}_{q^d} = \mathbb{F}_q[\alpha]$. Observe that the character χ_{q^d} is not trivial on $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^d}$. It follows from Wan [11, Corollary 2.2], taking $\beta = -\alpha$ in the notation of that paper, that

$$\left| \sum_{c \in \mathbb{F}_q} \chi_{q^d}(c + \alpha) \right| \leq (d-1) q^{1/2}.$$

Provided that $q > (d-1)^2$, one has $(d-1)q^{1/2} < q$, and thus the desired conclusion follows. □

We are now equipped to establish the final conclusion of Theorem 1.1.

Theorem 3.9. *Let d be an even integer, and suppose that q is an odd prime power with $q > (d-1)^2$. Then $s_2(q,d) = 0$.*

Proof. Suppose that $f(x) \in \mathbb{F}_q[x]$ is a 2-superirreducible polynomial of degree d over $\mathbb{F}_q$, and consider a root $\alpha \in \mathbb{F}_{q^d}$ of f. By Lemma 3.3, we must have $\chi_{q^d}(\alpha + c) = -1$ for every $c \in \mathbb{F}_q$, and hence

$$\sum_{c \in \mathbb{F}_q} \chi_{q^d}(\alpha + c) = -q.$$

This contradicts the estimate supplied by Lemma 3.8, since we have assumed that $q > (d-1)^2$. Consequently, there can be no 2-superirreducible polynomials of degree d over $\mathbb{F}_q$. □

4. Relationship to rational and p-adic superirreducibility

Fix a rational prime number p. Then, any monic polynomial $f \in \mathbb{Z}[x]$ that is irreducible modulo p is also irreducible over $\mathbb{Q}[x]$. One might guess that this familiar property extends from irreducibility to superirreducibility. Thus, if the monic polynomial $f(x)$ reduces to a weakly k-superirreducible polynomial modulo p, one might expect that $f(x)$ is itself weakly k-superirreducible over $\mathbb{Z}$, and perhaps also over $\mathbb{Q}$. We find that such an expectation is in fact excessively optimistic. Indeed, there are 2-superirreducible polynomials over $\mathbb{F}_3$ with integral lifts that are not 2-superirreducible over $\mathbb{Z}$.

Example 4.1. Consider the polynomial $f(x) \in \mathbb{Z}[x]$ given by

$$f(x) = x^4 - 12x^3 + 2x^2 - 39x + 71.$$

Then, we have $f(x) \equiv x^4 - x^2 - 1 \pmod 3$, and it is verified by an exhaustive check that $x^4 - x^2 - 1$ is 2-superirreducible in $\mathbb{F}_3[x]$. However, one has

$$f(3t^2 + t) = (t^4 + 3t^3 + 2t^2 - 1)(81t^4 - 135t^3 - 27t^2 + 39t - 71),$$

so that $f(x)$ is not 2-superirreducible over $\mathbb{Z}$.

Despite examples like the one above, one may still hope that the assumption of additional congruential properties involving higher powers of p might suffice to exclude such problematic examples, thereby providing a means to lift superirreducible polynomials over $\mathbb{Z}_p$ to superirreducible polynomials over $\mathbb{Z}$. The following proposition reveals a major obstruction to any such lifting process, since it shows that for each natural number $k \geq 2$, there are no p-adic weakly k-superirreducible polynomials.

Proposition 4.2. *Let p be a prime number. When $k \geq 2$, there are no weakly k-superirreducible polynomials over $\mathbb{Z}_p$ or over $\mathbb{Q}_p$.*

Proof. Suppose, if possible, that $f \in \mathbb{Q}_p[x]$ is a weakly k-superirreducible polynomial. There is no loss of generality in assuming that f is an irreducible polynomial lying in $\mathbb{Z}_p[x]$. Let α be a root of f lying in a splitting field extension for f over $\mathbb{Q}_p$, and let $e = 1 + |v_p(\alpha)|$, where $v_p(\alpha)$ is defined in such a manner that $|\alpha|_p = p^{-v_p(\alpha)}$. Let $h \in \mathbb{Z}_p[t]$ be any polynomial of degree k, put $g(t) = p^e h(t) + t$, and consider the equation $g(\beta) = \alpha$. Since $|g(\alpha) - \alpha|_p < 1$ and $|g'(\alpha)|_p = |1 + p^e h'(\alpha)|_p = 1$, an application of Hensel's lemma demonstrates that the equation $g(\beta) = \alpha$ has a solution $\beta \in \mathbb{Q}_p(\alpha)$. Thus, the equation $\alpha = p^e h(\beta) + \beta$ has a solution $\beta \in \mathbb{Q}_p(\alpha)$, and by appealing to Lemma 2.2, we conclude that the polynomial $f(p^e h(t) + t)$ is reducible over $\mathbb{Q}_p[t]$. Since $p^e h(t) + t \in \mathbb{Z}_p[t]$, we see that f is neither weakly k-superirreducible over $\mathbb{Z}_p$ nor over $\mathbb{Q}_p$, and we arrive at a contradiction. The desired conclusion follows. □

The discussion of this section appears to show, therefore, that superirreducibility over $\mathbb{F}_p$, and indeed superirreducibility over $\mathbb{Z}_p$ and $\mathbb{Q}_p$, is not closely connected to corresponding superirreducibility over $\mathbb{Z}$ and $\mathbb{Q}$.

5. Acknowledgements

We thank an anonymous referee for providing helpful comments on improving the clarity of the paper as well as for bringing to our attention the references [1,6,7]. We are grateful to the developers of Magma, Mathematica, and SageMath for writing software that we used to search for numerical examples and perform plausibility checks on asymptotics proved in this paper.

The fourth author is supported by NSF grant DMS-2302514. The fifth author is supported by NSF grants DMS-1854398 and DMS-2001549. The first, third, and fourth authors are also supported by the Heilbronn Institute for Mathematical Research.

REFERENCES

[1] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman, and T. J. Tucker, *Current trends and open problems in arithmetic dynamics*, Bull. Amer. Math. Soc. **56** (2019), no. 4, 611–685.

[2] J. W. Bober, D. Fretwell, G. Martin and T. D. Wooley, *Smooth values of polynomials*, J. Austral. Math. Soc. **108** (2020), no. 2, 245–261.

[3] L. Du, *Superirreducibility of polynomials, binomial coefficient asymptotics and stories from my classroom*, Ph.D. Thesis, University of Michigan, 2020.

[4] C. F. Gauss, *Untersuchungen über höhere Arithmetik*, Chelsea, New York, 1965.

[5] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer, New York, 1982.

[6] R. Jones and A. Levy, *Eventually stable rational functions*, Int. J. Number Theory **13** (2017), no. 9, 2299–2318.

[7] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. Lond. Math. Soc. (3) **51** (1985), no. 3, 385–414.

[8] A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith. **13** (1967), no. 2, 177–236.

[9] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000.

[10] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Math., vol. 536, Springer, New York, 1976.

[11] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), no. 219, 1195–1212.

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, FRY BUILDING, WOODLAND ROAD, BRISTOL BS8 1UG, UK AND THE HEILBRONN INSTITUTE FOR MATHEMATICAL RESEARCH, BRISTOL, UK
Email address: j.bober@bristol.ac.uk

DEPARTMENT OF MATHEMATICS, DRAPER BUILDING, BEREA COLLEGE, 101 CHESTNUT ST., BEREA, KY 40404, USA
Email address: dul@berea.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, FYLDE COLLEGE, LANCASTER UNIVERSITY, LANCASTER LA1 4YF, UK
Email address: d.fretwell@lancaster.ac.uk

DEPARTMENT OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, LOCKETT HALL, BATON ROUGE, LA 70803, USA
Email address: kopp@math.lsu.edu

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, 150 N. UNIVERSITY STREET, WEST LAFAYETTE, IN 47907-2067, USA
Email address: twooley@purdue.edu