THE DISTANCE TO A SQUAREFREE POLYNOMIAL OVER $\mathbb{F}_2[x]$

MICHAEL FILASETA AND RICHARD A. MOY

Abstract. In this paper, we examine how far a polynomial in $\mathbb{F}_2[x]$ can be from a squarefree polynomial. For any $\epsilon > 0$, we prove that for any polynomial $f(x) \in \mathbb{F}_2[x]$ with degree n, there exists a squarefree polynomial $g(x) \in \mathbb{F}_2[x]$ such that $\deg g \leq n$ and $L_2(f-g) < (\ln n)^{2\ln(2)+\epsilon}$ (where L_2 is a norm to be defined). As a consequence, the analagous result holds for polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$.

1. Introduction

In the 1960's, Pál Turán (cf. [11]) posed the problem of determining whether there is an absolute constant C such that for every polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, there is a polynomial $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ irreducible over the rationals satisfying $L(f-g) := \sum_{j=0}^{n} |b_j - a_j| \leq C$. It is currently known that the existence of such a C is connected to an open problem on covering systems of the integers with distinct odd moduli [5, 11]; if one allows $g(x)$ to have degree $> n$, then one can take $C = 3$ [1, 12]; for all $f(x)$ of degree ≤ 40 such a $g(x)$ exists with $C = 5$ [7]; for the corresponding problem in $\mathbb{F}_2[x]$, if C exists, then $C \geq 4$ [1]; and for the corresponding problem in $\mathbb{F}_p[x]$ with p an odd prime, if C exists, then $C \geq 3$ [6]. Other papers on this topic include [2, 7, 8, 9, 10]. In [6], a case is made for the following conjecture.

Conjecture 1.1. *For every $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 1$, there is an irreducible polynomial $g(x) \in \mathbb{Z}[x]$ of degree at most n satisfying $L(f-g) \leq 2$.*

In [4], Dubickas and Sha investigated an interesting variant of this conjecture where they asked how far a polynomial $f(x) \in \mathbb{Z}[x]$ can be from a squarefree polynomial, that is from a polynomial in $\mathbb{Z}[x]$ not divisible by the square of an irreducible polynomial over $\mathbb{Q}$.

Conjecture 1.2. *For every $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 0$, there is a squarefree polynomial $g(x) \in \mathbb{Z}[x]$ of degree at most n satisfying $L(f-g) \leq 2$.*

Among other nice results, Dubickas and Sha [4, Theorem 1.4] show that if $g(x)$ is allowed to have degree $> n$, then such a squarefree polynomial $g(x) \in \mathbb{Z}[x]$ exists satisfying $L(f-g) \leq 2$. They [4, Theorem 1.3] also show that for $n \geq 15$, there are infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ of degree n such that if $g(x) \in \mathbb{Z}[x]$ is squarefree, then $L(f-g) \geq 2$. We show in the next section that this latter result extends to k-free polynomials.

Theorem 1.3. *Let k be an integer ≥ 2. There exists a computable $N_0 = N_0(k)$ such that if $n \geq N_0$, then there are infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ of degree n such that if $g(x) \in \mathbb{Z}[x]$ is k-free, then $L(f-g) \geq 2$.*

Our argument for Theorem 1.3 gives as a permissible value of N_0 the number

$$N_0 = k \sum_{j=1}^{2k} (p_j - 1) + k + 1,$$

where $p_1, \ldots, p_{2k}$ are the first $2k$ primes. We expect much smaller N_0 will suffice.

One can approach the above conjectures by investigating the analogous questions for polynomials over finite fields. Indeed, this is done for Conjecture 1.1 in [2, 6, 7, 9, 10].

Definition 1.4. Let $\mathbb{F}_p$ be any finite field with p elements where p is a prime. For any polynomial $f(x) \in \mathbb{F}_p[x]$, define its *length* $L_p(f)$ by choosing each of its coefficients in the interval $(-p/2, p/2]$ and then summing their absolute values in $\mathbb{Z}$.

Using this definition of distance in $\mathbb{F}_p[x]$, Dubickas and Sha [4, Question 6.2] asked the following question.

Question 1.5. *For any prime number p and any polynomial $f(x) \in \mathbb{F}_p[x]$, is there a squarefree polynomial $g(x) \in \mathbb{F}_p[x]$ of degree at most $\deg f$ satisfying $L_p(f - g) \leq 2$?*

In this paper, we will prove the following theorem.

Theorem 1.6. *Fix $\epsilon > 0$. Let $f(x) \in \mathbb{F}_2[x]$ with $\deg f = n$. If n is sufficiently large, then there exists a squarefree polynomial $g(x) \in \mathbb{F}_2[x]$ of degree n such that*

$$L_2(f - g) \leq (\ln n)^{2\ln(2)+\epsilon}.$$

In the next section, we justify the following consequence of Theorem 1.6.

Corollary 1.7. *Fix $\epsilon > 0$. Let $f(x) \in \mathbb{Z}[x]$ with $\deg f = n$. If n is sufficiently large, then there exists a squarefree polynomial $g(x) \in \mathbb{Z}[x]$ of degree n such that*

$$L(f - g) \leq (\ln n)^{2\ln(2)+\epsilon}.$$

2. Proofs of Theorem 1.3 and Corollary 1.7

Before turning to our main result, we establish Theorem 1.3 and show that Corollary 1.7 is a consequence of Theorem 1.6.

Proof of Theorem 1.3. Fix a positive integer k. Let $\Phi_n(x)$ denote the nth cyclotomic polynomial. For distinct positive integers m and n, Diederichsen [3] obtained the value of the resultant $\mathrm{Res}(\Phi_n(x), \Phi_m(x))$. For our purposes, we only use that this resultant is 1 in the case that m and n are distinct primes. For monic polynomials $f(x)$ and $g(x)$, one can view the $|\mathrm{Res}(f(x), g(x))|$ as the product of $g(\alpha)$ as α runs through the roots of $f(x)$. It follows that for distinct primes p and q, we have

$$\mathrm{Res}(\Phi_p(x)^k, \Phi_q(x)^k) = \pm 1.$$

Furthermore, for any prime p, one can see that

$$\mathrm{Res}(x^k, \Phi_p(x)^k) = \pm 1.$$

Both of the above resultants hold with ± 1 replaced by 1, but this is not important to us.

Let $p_1, p_2, \ldots, p_{2k}$ be arbitrary distinct primes. Define

$$f_0(x) = x^k \quad \text{and} \quad f_j(x) = \Phi_{p_j}(x)^k \ \text{ for } 1 \leq j \leq 2k.$$

From the above, we have $\mathrm{Res}(f_i(x), f_j(x)) = \pm 1$ for distinct i and j in $\{0, 1, \ldots, 2k\}$. The significance of this is that as a consequence each $f_i(x)$ has an inverse modulo $f_j(x)$ in $\mathbb{Z}[x]$. Thus, a Chinese Remainder Theorem argument implies that for arbitrary $a_j(x) \in \mathbb{Z}[x]$, there is a $g(x) \in \mathbb{Z}[x]$ that satisfies

$$g(x) \equiv a_j(x) \pmod{f_j(x)}, \quad \text{for all } j \in \{0, 1, \ldots, 2k\}.$$

We set

$$a_0 = 0 \quad \text{and} \quad a_j(x) = (-1)^j x^{\lfloor (j-1)/2 \rfloor} \text{ for } 1 \leq j \leq 2k.$$

Then $g(x)$ above has the property that $g(x) - (-1)^j x^{\lfloor (j-1)/2 \rfloor}$ is divisible by $f_j(x) = \Phi_{p_j}(x)^k$ for $1 \leq j \leq 2k$. Furthermore, for any $\ell \geq k$, the condition $a_0 = 0$ implies $g(x)$ and $g(x) \pm x^\ell$ are divisible by x^k. Taking N equal to the degree of

$$P(x) = \prod_{1 \leq j \leq 2k} \Phi_{p_j}(x)^k,$$

we can find $g(x)$ as above of degree $< N + k$. Then for $n \geq N_0 := N + k + 1$ and arbitrary integers a and b, the polynomial

$$F(x) = g(x) + x^{n-N-1} P(x)(ax + b)$$

of degree n has the property that if $h(x) \in \mathbb{Z}[x]$ and $L(F - h) \leq 1$, then $h(x)$ is divisible by one of the $f_j(x)$ and, hence, not k-free. The role of the expression $ax + b$ in the definition of $F(x)$ is to clarify that for a given $n \geq N_0$, there are infinitely many possibilities for $F(x)$, completing the proof of Theorem 1.3. $\square$

Proof of Corollary 1.7 assuming Theorem 1.6. We consider $\epsilon > 0$ and n sufficiently large. Let $f_2(x) = f(x)$ if the leading coefficient of $f(x)$ is odd; otherwise, let $f_2(x) = f(x) + x^n$. Thus, in either case, $f_2(x)$ has degree n and an odd leading coefficient. Let $\bar{f}_2(x)$ be a $0,1$-polynomial (a polynomial all of whose coefficients are 0 or 1) satisfying $\bar{f}_2(x) \equiv f_2(x) \pmod 2$. By Theorem 1.6, there is a $0,1$-polynomial $\bar{g}_2(x)$, squarefree in $\mathbb{F}_2[x]$, such that

$$L(\bar{f}_2 - \bar{g}_2) = L_2(\bar{f}_2 - \bar{g}_2) < (\ln n)^{2\ln(2) + \epsilon/2}.$$

Furthermore, $\bar{g}_2(x)$ has degree n and, hence, an odd leading coefficient of 1. Observe that there is a $g_2(x) \in \mathbb{Z}[x]$ with $g_2(x) \equiv \bar{g}_2(x) \pmod 2$ and with each coefficient of $f_2(x) - g_2(x)$ in $\{0, 1\}$. In particular, $g_2(x)$ has degree n, and we see that

$$L(f - g_2) \leq 1 + L(f_2 - g_2) = 1 + L(\bar{f}_2 - \bar{g}_2) \leq 1 + (\ln n)^{2\ln(2) + \epsilon/2} \leq (\ln n)^{2\ln(2) + \epsilon},$$

completing the proof. $\square$

3. Preliminaries to Theorem 1.6

Unless stated otherwise, we restrict our attention to arithmetic over $\mathbb{F}_2$, the field with two elements. In addition to the notation discussed in the previous section, we define the degree of a 0 polynomial to be $-\infty$ with the understanding that $\deg 0 = -\infty < \deg w$ for non-zero $w(x) \in \mathbb{F}_2[x]$.

Our approach to proving Theorems 1.6 relies on the following idea from [4]. If $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{F}_2[x]$ has degree n, then we define

$$f_e(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_{2i} x^i \quad \text{and} \quad f_o(x) = \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_{2i+1} x^i.$$

Observe that $f(x) = (f_e(x))^2 + x(f_o(x))^2$. Further observe that $f'(x) = (f_o(x))^2$. As noted in [4, Lemma 5.1], we have the following lemma.

Lemma 3.1. *Let $f(x) \in \mathbb{F}_2[x]$ with degree at least 2. The polynomial $f(x)$ is squarefree in $\mathbb{F}_2[x]$ if and only if $\gcd(f_e(x), f_0(x)) = 1$. Moreover, any irreducible polynomial appearing as a factor of $f(x)$ to a multiplicity > 1 is a factor of the polynomial $\gcd(f_e(x), f_o(x))$.*

This lemma will be crucial to our result. Observe that Lemma 3.1 allows one to view a polynomial $f(x) \in \mathbb{F}_2[x]$ of degree n as an ordered pair of polynomials of degree at most $n/2$. Finding a nearby squarefree polynomial of degree n is tantamount to finding a nearby ordered pair of polynomials which have trivial gcd.

We also make use of the following result.

Lemma 3.2. *Let $n \in \mathbb{Z}^+$, and let p be a prime. The degree of the product of the monic irreducible polynomials of degree $\leq n$ in $\mathbb{F}_p[x]$ is less than or equal to $p(p^n - 1)/(p - 1)$.*

Proof. Every irreducible polynomial in $\mathbb{F}_p[x]$ of degree n divides $x^{p^n} - x$. Hence, the degree of the product of the monic irreducible polynomials of degree n is less than or equal to p^n. Since $p + p^2 + \cdots + p^n = p(p^n - 1)/(p - 1)$, the result follows. □

Next, we bound the minimum distance between a polynomial f and a multiple of a polynomial d.

Lemma 3.3. *Let $f(x), d(x) \in \mathbb{F}_2[x]$ with $\deg d > 0$. There exists a polynomial $g(x) \in \mathbb{F}_2[x]$ of degree at most $\deg f$ such that $d(x)|g(x)$ and $L_2(f - g) \leq \deg d$. Furthermore, if also $\deg d \leq \deg f$, then one can take $\deg g = \deg f$.*

Proof. There exist polynomials $q(x), r(x) \in \mathbb{F}_2[x]$ such that $f(x) = d(x)q(x) + r(x)$, $\deg r < \deg d$, and $\deg(d(x)q(x)) \leq \deg f$, with equality if $\deg d \leq \deg f$. Since

$$L_2(f(x) - d(x)q(x)) \leq \deg d,$$

we can take $g(x) = d(x)q(x)$ to complete the proof. □

By taking $g(x) = d(x)q(x) + 1$ in the argument above, we obtain the following.

Lemma 3.4. *Let $f(x), d(x) \in \mathbb{F}_2[x]$ with $f(x)$ non-zero and $\deg d > 0$. There exists a polynomial $g(x) \in \mathbb{F}_2[x]$ of degree at most $\deg f$ such that $\gcd(d, g) = 1$ and $L_2(f - g) \leq \deg d$. Furthermore, if also $\deg d \leq \deg f$, then one can take $\deg g = \deg f$.*

Here is another lemma that will prove useful later.

Lemma 3.5. *For t a positive integer, set $\Pi_1 = \prod_{i=1}^{t} (x^i + 1) \in \mathbb{F}_2[x]$, and let $\tilde{\Pi}_1$ be the product of the distinct irreducible polynomials dividing Π_1. The degree of $\tilde{\Pi}_1$ is $\leq \lceil t/2 \rceil^2 - \lceil t/2 \rceil + 1$.*

Proof. Each factor x^i+1 in Π_1 is divisible by $x+1$. Furthermore, if i is even, then $x^i+1 = (x^{i/2}+1)^2$ and thus does not contribute new irreducible factors to $\tilde{\Pi}_1$. In other words,

$$\begin{aligned}\deg\left(\tilde{\Pi}_1\right) &\le 1 + \deg\left(\prod_{i=1}^{\lceil t/2\rceil} \frac{x^{2i-1}+1}{x+1}\right)\\ &= 1+2+4+6+\cdots+(2\lceil t/2\rceil-2)\\ &= 1+2\big(1+2+3+\cdots+(\lceil t/2\rceil-1)\big)\\ &= 1+\left(\left\lceil\frac{t}{2}\right\rceil-1\right)\left\lceil\frac{t}{2}\right\rceil,\end{aligned}$$

from which the lemma follows. □

We immediately have the following corollary.

Corollary 3.6. *Let t be an integer ≥ 2. Set $\Pi_2 = x\prod_{i=1}^{t}(x^i+x^{i-1}+\cdots+x+1)\in\mathbb{F}_2[x]$, and let $\tilde{\Pi}_2$ be the product of the distinct irreducible polynomials dividing Π_2. The degree of $\tilde{\Pi}_2$ is $\le \lceil (t+1)/2\rceil^2$.*

4. A proof of Theorem 1.6

To prove Theorem 1.6, we begin with a few technical lemmas.

Lemma 4.1. *Fix $\epsilon\in(0,1)$, and let n be a positive integer $\ge n_0(\epsilon)$ where $n_0(\epsilon)$ is sufficiently large. Set $t=\lceil 2\ln(\log_2 n)/(1-\epsilon)\rceil\in\mathbb{N}$. Let Π_2 be as in Corollary 3.6. Let $f(x)\in\mathbb{F}_2[x]$ with $\gcd(f(x),\Pi_2)=1$ and $\deg f\le n$. Set*

$$P(x) = P_\epsilon(x) = \prod_{\substack{p(x)\in\mathbb{F}_2[x] \text{ irreducible}\\ \deg p\le t\\ p(x)\nmid f(x)}} p(x).$$

Then the polynomials in the collection

$$\{f(x)+a(x)P(x)\},\quad \text{where}\quad a(x)\in\{1, x+1, x^2+x+1,\dots,x^t+x^{t-1}+\cdots+x+1\},$$

have no irreducible factors of degree $\le t$. Furthermore, the polynomials in this collection are pairwise coprime.

Proof. Let $p(x)$ be an irreducible polynomial of degree $\le t$. Then $p(x)|f(x)$ or $p(x)|P(x)$, but not both. If $p(x)|P(x)$, then $p(x)\nmid f(x)$ so that $p(x)\nmid \big(f(x)+a(x)P(x)\big)$. If $p(x)|f(x)$ then $p(x)\nmid P(x)$. In this case, since $p(x)|f(x)$ and $\gcd(f(x),\Pi_2)=1$, we deduce that $\gcd(p(x),a(x))=1$. Therefore, $p(x)\nmid \big(f(x)+a(x)P(x)\big)$. Thus, the polynomials of the form $f(x)+a(x)P(x)$, as defined above, have no irreducible factors of degree $\le t$.

We deduce then that the polynomials of the form $f(x)+a(x)P(x)$ are pairwise relatively prime since they have no irreducible factors of degree less than or equal to t and the difference of any two distinct $f(x)+a(x)P(x)$ is divisible only by irreducible polynomials of degree less than or equal to t. □

Lemma 4.2. *Fix $\epsilon \in (0,1)$, and let n be a positive integer $\geq n_0(\epsilon)$ where $n_0(\epsilon)$ is sufficiently large. Let $t = \lceil 2\ln(\log_2 n)/(1-\epsilon)\rceil \in \mathbb{N}$. Suppose that $f_0(x), f_1(x), \dots, f_t(x) \in \mathbb{F}_2[x]$ are polynomials of degree $\leq n$ which are also pairwise relatively prime and have no irreducible factors of degree $\leq t$. If $g(x) \in \mathbb{F}_2[x]$ has degree $\leq n$, then there exists a polynomial $g_1(x) \in \mathbb{F}_2[x]$ with $\deg g_1 \leq n$ such that $L_2(g - g_1) \leq \log_2 n$ and, for some $i \in \{0, 1, 2, \dots, t\}$, we have $\gcd(g_1, f_i) = 1$. Furthermore, if $\deg g \geq \log_2 n$, then we may take $\deg g_1 = \deg g$.*

Proof. We proceed by adjusting the coefficients of $g(x)$ in the terms of degree $< \log_2 n$ to produce the desired $g_1(x)$. Observe that there are at least $2^{\log_2 n} = n$ such possibilities for $g_1(x)$. Furthermore, if $\deg g \geq \log_2 n$, then each such $g_1(x)$ satisfies $\deg g_1 = \deg g$. We examine the possible irreducible polynomials $w(x)$ which can divide $\gcd(g_1, f_i)$. By the assumptions on the $f_i(x)$, we see that $\deg w > t$.

We consider now two cases depending on whether (i) $t < \deg w \leq \log_2 n$ or (ii) $\deg w > \log_2 n$. After considering both cases, we combine information from the two cases to obtain the desired result.

Case (i): Let $d = \deg w$. For each fixed choice of the coefficients, say $a_j \in \{0,1\}$, of x^j in $g_1(x)$ for $j \in \{d, d+1, \dots, \lfloor \log_2 n \rfloor\}$, there is at most one choice of the coefficients $a_j \in \{0,1\}$ of x^j in $g_1(x)$ for $j \in \{0, 1, \dots, d-1\}$ such that $g_1(x)$ is divisible by $w(x)$. Thus, such a $w(x)$ divides at most $2^{(\log_2 n)-d+1}$ possibilities for $g_1(x)$.

Since every irreducible polynomial in $\mathbb{F}_2[x]$ of degree d divides $x^{2^d} - x$, there are at most $2^d/d$ irreducible polynomials of degree d in $\mathbb{F}_2[x]$. Therefore, there are at most

$$\frac{2^d}{d} \times 2^{(\log_2 n)-d+1} = \frac{2n}{d}$$

possibilities for $g_1(x)$ that are divisible by an irreducible polynomial of degree d. By summing over d in the range $(t, \log_2 n]$, we deduce that there are at most

$$\sum_{t<d\leq \log_2 n} \frac{2n}{d} \leq 2n\left(\ln(\log_2 n) - \ln(t) + O\left(\frac{1}{t}\right)\right) \leq 2n\ln(\log_2 n)$$

possibilities for $g_1(x)$ having an irreducible factor $w(x)$ as in (i). As this estimate is $> n$, we need to revise this estimate. We explain next how to reduce the above estimate by a factor of $t+1$.

Recall that we are wanting $\gcd(g_1, f_i) = 1$ for some $i \in \{0, 1, 2, \dots, t\}$ rather than for every such i. We choose the $i \in \{0, 1, 2, \dots, t\}$ that minimizes the number of possibilities for $g_1(x)$ which are divisible by an irreducible $w(x) \in \mathbb{F}_2[x]$ with $\deg w \in \big(t, \log_2 n\big]$ and $w(x)|f_i(x)$. Since the $f_j(x)$ are pairwise relatively prime, we deduce that the number of possibilities for $g_1(x)$ with $\gcd(g_1, f_i)$ divisible by an irreducible $w(x) \in \mathbb{F}_2[x]$ of degree $d \in \big(t, \log_2 n\big]$ is at most

$$\frac{1}{t+1}\sum_{t<d\leq \log_2 n} \frac{2n}{d} \leq \frac{2n\ln(\log_2 n)}{t+1} \leq (1-\epsilon)n.$$

We proceed now to Case (ii) with this choice of i.

Case (ii): In this case, we use that an irreducible polynomial with degree $> \log_2 n$ can divide at most one possibility for $g_1(x)$. With i as in Case (i), we see that $f_i(x)$ can have at most $n/\log_2 n$ distinct irreducible factors of degree greater than $\log_2 n$. Therefore, at most $n/\log_2 n$ possibilities for $g_1(x)$ have an irreducible factor of degree greater than $\log_2 n$ in common with $f_i(x)$.

By combining our estimates from Case (i) and (ii), we deduce that there is some $f_i(x)$ such that there are at most

$$(1-\epsilon)n + \frac{n}{\log_2 n}$$

possibilities for $g_1(x)$ that share a non-constant factor with f_i. Therefore, with $n \geq n_0(\epsilon)$, there exists a $g_1(x) \in \mathbb{F}_2[x]$ with $\deg g_1 \leq n$ such that $L_2(g - g_1) \leq \log_2 n$ and $\gcd(g_1, f_i) = 1$ for some $i \in \{0, 1, \ldots, t\}$. □

Now we proceed with the proof of Theorem 1.6.

Proof of Theorem 1.6. We take n sufficiently large as stated in the theorem, and set $\epsilon' = \epsilon/(\epsilon + 4\ln 2)$. Let $t = \lceil 2\ln(\log_2 n)/(1-\epsilon') \rceil \in \mathbb{N}$, and let Π_2 be as in Corollary 3.6. From Corollary 3.6, we see that $\deg(\tilde{\Pi}_2) \leq \lceil (t+1)/2 \rceil^2$. We apply Lemma 3.4 using the polynomials $f_e(x)$ and $\tilde{\Pi}_2$ to deduce that there exists $\tilde{f}(x)$ with $\deg \tilde{f} \leq \lfloor n/2 \rfloor$ and $\gcd(\tilde{f}(x), \Pi_2) = 1$ such that

$$L_2(f_e - \tilde{f}) \leq \lceil (t+1)/2 \rceil^2.$$

Furthermore, if $\deg f_e \geq \lceil (t+1)/2 \rceil^2$, we can take $\deg \tilde{f} = \deg f_e$ and do so. Define $P(x) = P_{\epsilon'}(x)$ as in Lemma 4.1. By this lemma, the polynomials in $\{\tilde{f}(x) + a(x)P(x)\}$, where $a(x) \in \{1, x+1, x^2+x+1, \ldots, x^t + x^{t-1} + \cdots + x + 1\}$, have no irreducible factors of degree $\leq t$. Furthermore, the polynomials in this collection are pairwise coprime. For $i \in \{0, 1, \ldots, t\}$, set $\tilde{f}_i = \tilde{f} + (x^i + x^{i-1} + \cdots + x + 1)P(x)$. Since $\tilde{f}_i$ has no irreducible factor of degree $\leq t$, we have in particular that $\tilde{f}_i(0) \neq 0$. From Lemma 3.2, we see that

$$L_2(\tilde{f} - \tilde{f}_i) \leq \deg(\tilde{f} - \tilde{f}_i) \leq t + 2\big(2^t - 1\big) < t + 4(\log_2 n)^{2\ln(2)+\epsilon/2}, \quad \text{for } 0 \leq i \leq t.$$

By Lemma 4.2, there is a polynomial $\tilde{g}_1(x)$ with $\deg \tilde{g}_1 \leq \lfloor (n-1)/2 \rfloor$ such that $L_2(\tilde{g}_1 - f_o) \leq \log_2 n$ and $\gcd(\tilde{g}_1, f_i) = 1$ for some $i \in \{0, 1, \ldots, t\}$. Furthermore, we take as we can $\deg \tilde{g}_1 = \deg f_o$ if $\deg f_0 \geq \log_2 n$. With i so fixed, we set $g(x) = \tilde{f}_i(x)^2 + x\tilde{g}_1(x)^2$. Observe that $\deg g \leq n$ and $g(x)$ is squarefree by Lemma 3.1. The condition $\deg f = n$ implies that $\deg f_i = \deg f_e$ or $\deg \tilde{g}_1 = \deg f_o$ with both holding if $\deg f_e$ and $\deg f_o$ are both $\geq \max\{\log_2 n, \lceil (t+1)/2 \rceil^2\}$. This implies $\deg g = \deg f = n$. The estimate

$$\begin{aligned}
L_2(f-g) &= L_2(\tilde{f}_i^2 - f_e^2) + L_2(\tilde{g}_1^2 - f_o^2) \\
&= L_2(\tilde{f}_i - f_e) + L_2(\tilde{g}_1 - f_o) \\
&\leq L_2(f_e - \tilde{f}) + L_2(\tilde{f} - \tilde{f}_i) + L_2(\tilde{g}_1 - f_o) \\
&\leq \left\lceil \frac{t+1}{2} \right\rceil^2 + t + 4(\log_2 n)^{2\ln(2)+\epsilon/2} + \log_2 n < (\ln n)^{2\ln(2)+\epsilon}
\end{aligned}$$

completes the proof of the theorem. □

References

[1] Pradipto Banerjee and Michael Filaseta. On a polynomial conjecture of Pál Turán. *Acta Arith.*, 143(3):239–255, 2010.

[2] A. Bérczes and L. Hajdu. Computational experiences on the distances of polynomials to irreducible polynomials. *Math. Comp.*, 66(217):391–398, 1997.

[3] Fritz-Erdmann Diederichsen. Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz. *Abh. Math. Sem. Hansischen Univ.*, 13:357–412, 1940.

[4] Artūras Dubickas and Min Sha. The distance to square-free polynomials. *Acta Arith.*, 186(3):243–256, 2018.

[5] Michael Filaseta. Coverings of the integers associated with an irreducibility theorem of A. Schinzel. In *Number theory for the millennium, II (Urbana, IL, 2000)*, pages 1–24. A K Peters, Natick, MA, 2002.

[6] Michael Filaseta. Is every polynomial with integer coefficients near an irreducible polynomial? *Elem. Math.*, 69(3):130–143, 2014.

[7] Michael Filaseta and Michael J. Mossinghoff. The distance to an irreducible polynomial, II. *Math. Comp.*, 81(279):1571–1585, 2012.

[8] K. Győry. On the irreducibility of neighbouring polynomials. *Acta Arith.*, 67(3):283–294, 1994.

[9] Gilbert Lee, Frank Ruskey, and Aaron Williams. Hamming distance from irreducible polynomials over $\mathbb{F}_2$. In *2007 Conference on Analysis of Algorithms, AofA 07*, Discrete Math. Theor. Comput. Sci. Proc., AH, pages 169–180. Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2007.

[10] Michael J. Mossinghoff. The distance to an irreducible polynomial. In *Gems in experimental mathematics*, volume 517 of *Contemp. Math.*, pages 275–288. Amer. Math. Soc., Providence, RI, 2010.

[11] A. Schinzel. Reducibility of polynomials and covering systems of congruences. *Acta Arith.*, 13:91–101, 1967/1968.

[12] A. Schinzel. Reducibility of lacunary polynomials. II. *Acta Arith.*, 16:371–392, 1969/1970.

University of South Carolina, Department of Mathematics, Columbia, SC 29208
E-mail address: filaseta@math.sc.edu

Lee University, Department of Mathematical Sciences, Cleveland, TN 37320
E-mail address: rmoy@leeuniversity.edu