ISSN 2590-9770
The Art of Discrete and Applied Mathematics 2 (2019) #P1.10
https://doi.org/10.26493/2590-9770.1330.993
(Also available at http://adam-journal.eu)

Polynomials of degree 4 over finite fields representing quadratic residues*

Shaofei Du [†]
Capital Normal University, School of Mathematical Sciences,
Bejing 100048, People's Republic of China

Klavdija Kutnar [‡]
University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia

Dragan Marušič [§]
University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia
IMFM, Jadranska 19, 1000 Ljubljana, Slovenia

Received 29 September 2019, accepted 13 October 2019, published online 30 December 2019

Abstract

It is proved that in a finite field F of prime order p, where p is not one of finitely many exceptions, for every polynomial $f(x) \in F[x]$ of degree 4 that has a nonzero constant term and is not of the form $\alpha g(x)^2$ there exists a primitive root $\beta \in F$ such that $f(\beta)$ is a quadratic residue in F. This refines a result of Madden and Vélez from 1982 about polynomials that represent quadratic residues at primitive roots.

Keywords: Finite field, polynomial, quadratic residues.

Math. Subj. Class.: 12E99

[*] The authors wish to thank Ademir Hujdurović and Kai Yuan for helpful conversations about the material of this paper.

[†] This work is supported in part by the National Natural Science Foundation of China (11671276).

[‡] Corresponding author. This work is supported in part by the Slovenian Research Agency (research program P1-0285 and research projects N1-0038, N1-0062, J1-6720, J1-6743, J1-7051, J1-9110, J1-1695, and J1-1715).

[§] This work is supported in part by the Slovenian Research Agency (I0-0035, research program P1-0285 and research projects N1-0038, N1-0062, J1-6720, J1-9108, and J1-1695), and in part by H2020 Teaming InnoRenew CoE (grant no. 739574).

E-mail addresses: dushf@mail.cnu.edu.cn (Shaofei Du), klavdija.kutnar@upr.si (Klavdija Kutnar), dragan.marusic@upr.si (Dragan Marušič)

1 Introduction

The motivation for this paper is twofold: first refining the result of Madden and Vélez about polynomials that represent quadratic residues at primitive roots [9], and in doing so obtaining a tool with which hamiltonicity of certain families of vertex-transitive graphs of order a product of two primes is proved via a structural analysis of their quotients with respect to an automorphism of prime order. Such a connection between algebraic graph theory and finite fields is not surprising, see, for example, [6, 14] for a similar application of finite fields.

In 1969 Lovász [8] asked for a construction of a finite connected vertex-transitive graph without a Hamilton path, that is, a path containing all vertices of the graph. This problem has spurred quite a bit of interest in the mathematical community, resulting in a number of papers affirming the existence of Hamilton paths and in some cases even Hamilton cycles (see the survey paper [7]). The main obstacle to making a substantial progress with regards to this problem is a lack of structural results for such graphs. Consequently, tools and methods from other areas of mathematics applicable in this context are more than welcome. Such is, for example, the case with the so-called polycirculant conjecture which states that every 2-closed group contains a fixed-point-free automorphism of prime order (see, for example, [3, 4, 10, 12, 13]). Fixed-point-free automorphism of prime order have been of great practical use in constructions of Hamilton cycles in vertex-transitive graphs via the so-called lifting cycle technique [1, 11]. And it is precisely here that the results of this paper are of crucial importance as they allow a successful application of this technique for a complete solution of Lovász problem for connected vertex-transitive graphs of order a product of two primes (see [5]).

More precisely, the goal of this paper is to obtain a novel result on polynomials of degree 4 over finite fields of prime order with regards to a polynomial representation of quadratic residues at primitive roots, thus refining results from [9] (see Theorem 1.1). (The set of nonzero quadratic residues modulo r, that is, nonzero elements of a finite field F of order r that are congruent to a perfect square modulo r, will be called *squares*.)

Theorem 1.1. *Let F be a finite field of prime order p, where p is an odd prime not given in Tables 1 and 2. Then for every polynomial $f(x) \in F[x]$ of degree 4 that has a nonzero constant term and is not of the form $\alpha g(x)^2$ there exists a primitive root $\beta \in F$ such that $f(\beta)$ is a square in F.*

2 Polynomials of degree 4 over finite fields representing quadratic residues

In early eighties, motivated by a question posed by Alspach, Heinrich and Rosenfeld [2] in the context of decompositions of complete symmetric digraphs, Madden and Vélez [9] investigated polynomials that represent quadratic residues at primitive roots. They proved that, with finally many exceptions, for any finite field F of odd characteristic, for every polynomial $f(x) \in F[x]$ of degree $r \geq 1$ not of the form $\alpha g(x)^2$ or $\alpha x g(x)^2$, there exists a primitive root β such that $f(\beta)$ is a nonzero square in F. It is the purpose of this paper to refine their result for polynomials of degree 4. This will then be used in [5] in the constructions of Hamilton cycles for some of the basic orbital graphs arising from the action of $\mathrm{PSL}(2, p)$ on cosets of D_{p-1}. This refinement, stated in Theorem 1.1, will be proved following a series of lemmas.

The following result, proved in [9], is a basis of our argument and will be used throughout this section.

Proposition 2.1 ([9, Corollary 1]). *Let F be a finite field with p^n elements. If s and t are integers such that*

(i) s and t are coprime,

(ii) a prime q divides $p^n - 1$ if and only if q divides st, and

(iii) $2\phi(t)/t > 1 + (rs - 2)p^{n/2}/(p^n - 1) + (rs + 2)/(p^n - 1)$,

then, given any polynomial $f(x) \in F[x]$ of degree r, square-free and with nonzero constant term, there exists a primitive root $\gamma \in F$ such that $f(\gamma)$ is a nonzero square in F.

Throughout this section let p be an odd prime and let $q_1 = 2, q_2, \ldots, q_m$ be the increasing sequence of prime divisors of $p - 1 = q_1^{i_1} q_2^{i_2} \cdots q_m^{i_m}$. As in [9] we define the following functions with respect to this sequence:

$$d(n, m) = 2\left(1 - \frac{1}{q_n}\right)\left(1 - \frac{1}{q_{n+1}}\right) \cdots \left(1 - \frac{1}{q_m}\right), \tag{2.1}$$

$$c_r(n, m) = 2r\sqrt{\frac{q_1 q_2 \cdots q_{n-1}}{q_n q_{n+1} \cdots q_m}}, \tag{2.2}$$

and $k(m)$ as the unique integer such that $d(k(m) - 1, m) \leq 1 < d(k(m), m)$. Hence $k(m) \geq 2$. Analogously the functions d and c_r can be defined for any positive integers $r \geq 1$, $n < m$ and an arbitrary sequence $\{q_1, \ldots, q_m\}$ of primes. The following lemma is a generalization of [9, Lemma 3].

Lemma 2.2. *Let $\{2 = q_1, q_2, \ldots, q_m\}$ be a finite sequence of primes satisfying $m \geq 2k(m) + 2$, and let $r = 4$. Then*

$$d(k(m) + 1, m) - c_r(k(m) + 1, m) > 1. \tag{2.3}$$

Proof. Since $2 \leq k(m) \leq \frac{m}{2} - 1$, we have $m \geq 6$. Since

$$d(k(m) + 1, m) = \left(1 + \frac{1}{q_{k(m)} - 1}\right) d(k(m), m) > 1 + \frac{1}{q_{k(m)} - 1},$$

(2.3) holds if

$$1 + \frac{1}{q_{k(m)} - 1} - 2r\left(\frac{q_1 q_2 \cdots q_{k(m)}}{q_{k(m)+1} q_{k(m)+2} \cdots q_m}\right)^{\frac{1}{2}} > 1,$$

which may be rewritten in the following form

$$q_2 q_3 \cdots q_{k(m)} (q_{k(m)} - 1)^2 < \frac{1}{128} q_{k(m)+1} \cdots q_{m-1} q_m, \tag{2.4}$$

in view of the fact that $r = 4$ and $q_1 = 2$.

We divide the proof into two cases, depending on whether $m \geq 7$ or $m = 6$.

Case 1. $m \geq 7$.

Let Ω be the increasing sequence of all prime numbers and let

$$\mathcal{J}_q = \{q_1 = 2, q_2, q_3, \ldots, q_l = q, q_{l+1}, \ldots, q_m\}$$

be a subsequence of Ω. Then we shall in fact prove a more general result:

$$q_2 q_3 \cdots q_l (q_l - 1)^2 < \frac{1}{128} q_{l+1} \cdots q_{m-1} q_m,$$

where $m \geq 7$ and $l \leq \frac{m}{2} - 1$ is any integer. To show this for the sequence $\mathcal{J}_q$ we define a subsequence $\mathcal{I}_q = \{w_1 = 2, w_2, w_3, \ldots, w_l = q, w_{l+1}, \ldots, w_m\}$ of Ω not missing any prime in Ω from the interval $[w_2, w_m]$. Then the lemma will be proven in case we show that the following holds:

$$w_2 w_3 \cdots w_l (w_l - 1)^2 < \frac{1}{128} w_{l+1} \cdots w_{m-1} w_m, \tag{2.5}$$

where $m \geq 7$ and $l \leq \frac{m}{2} - 1$ is any integer. If $w_m \geq 128$, then (2.5) is clearly true. So we only need to consider primes that are smaller than or equal to 127. If

$$(m - l) - (l - 1 + 2) = m - 2l - 1 \geq 2, \tag{2.6}$$

then (2.5) holds provided $w_{m-1} w_m > 128$ holds. Note that this is true if $w_m \geq 13$, which is the case since $m \geq 7$. Next, note that for either m being even and $l < \frac{m}{2} - 2$ or m being odd, (2.6) holds. So we may assume that m is even and that $l = m/2 - 1 \geq 2$.

Now we prove that (2.5) holds under this assumption for any even integer $m \geq 8$ by induction. Suppose first that $m = 8$. Then $l = 3$ and (2.5) rewrites as

$$w_2 w_3 (w_3 - 1)^2 < \frac{1}{128} w_4 w_5 w_6 w_7 w_8. \tag{2.7}$$

A computer search shows that (2.7) holds for all primes $w_8 \leq 127$. Suppose now that (2.5) is true for an even integer $m \geq 8$. Then we have

$$\begin{aligned} w_2 w_3 w_4 \cdots w_l w_{l+1} (w_{l+1} - 1)^2 &= w_2 (w_3 \cdots w_l w_{l+1} (w_{l+1} - 1)^2) \\ &< w_2 (w_{l+2} w_{l+3} \cdots w_m w_{m+1}) \\ &< (w_{l+2} w_{l+3} \cdots w_m w_{m+1}) w_{m+2}. \end{aligned}$$

Therefore (2.5) is true for all even integers $m \geq 8$ and then for all integers $m \geq 7$. Hence (2.4) holds, and so does (2.3).

Case 2. $m = 6$.

Now $k(m) = 2$. Inserting $l = 2$ and $m = 6$ in (2.5), we have

$$w_2 (w_2 - 1)^2 < \frac{1}{128} w_3 w_4 w_5 w_6. \tag{2.8}$$

A computer search for all the primes less than 131 shows that (2.8) does not hold only for

$$w_{k(m)} = w_2 \in \{11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 59, 61, 67, 71\}.$$

For these exceptional cases, we go back to work on (2.3) directly. Let $l = k(m) = 2$ in $\mathcal{J}_q$. Let $d(n, m)'$ and $c_4(n, m)'$ be the corresponding values for $\mathcal{I}_q$ as defined by functions d and c_r in (2.1) and (2.2). Then one can easily see that $d(3, 6)' \le d(3, 6)$ and that $c_4(3, 6)' \ge c_4(3, 6)$, which implies $d(3, 6) - c_4(3, 6) \ge d(3, 6)' - c_4(3, 6)'$. Therefore, (2.3) holds for $\mathcal{J}_q$ if it holds for $\mathcal{I}_q$. So it suffices to check (2.3) for $\mathcal{I}_q$. In fact, an additional computer search for the set of primes less than 131 shows that for $w_1 = 2$ and w_2 being each of these exceptional cases, (2.3) holds for $\mathcal{I}_q$. This completes the proof of Lemma 2.2. □

The following result proved in [9] will be needed in the next lemma.

Proposition 2.3 ([9, Lemma 5])**.** *Let $\{2 = q_1, q_2, \dots, q_m\}$ be a finite sequence of primes satisfying $m \le 2k(m) + 1$. Then $m \le 9$ and $q_{k(m)-1} \le 5$. In fact the sequence must satisfy one of the following:*

(i) $k(m) = 4$, $q_{k(m)-1} = 5$ *and* $m = 9$,

(ii) $k(m) = 3$, $q_{k(m)-1} = 5$ *and* $m \le 7$,

(iii) $k(m) = 3$, $q_{k(m)-1} = 3$ *and* $m \le 7$, *or*

(iv) $k(m) = 2$, $q_{k(m)-1} = 2$ *and* $m \le 5$.

Lemma 2.4. *Let $\{2 = q_1, q_2, \dots, q_m\}$ be a finite sequence of primes satisfying $m \le 2k(m) + 1$, and let $p - 1 = q_1^{i_1} q_2^{i_2} \cdots q_m^{i_m}$ with $q_m \ge 131$. Then there exist s and t such that*

(i) *s and t are coprime,*

(ii) *a prime q divides $p - 1$ if and only if q divides st, and*

(iii) $2\phi(t)/t > 1 + (4s - 2)\sqrt{p}/(p - 1) + (4s + 2)/(p - 1)$.

Proof. Since $m \le 2k(m) + 1$ the four cases (i) – (iv) of Proposition 2.3 need to be considered. In each case, as in [9, Lemma 7], we will prescribe a choice for s (which then determines t uniquely) and use the conditions in each of these four cases to find the lower bound α for the expression $(2\phi(t)t^{-1} - 1)$, that is, $(2\phi(t)t^{-1} - 1) \ge \alpha$. We will then be able to use the assumption $q_m \ge 131$ to show that

$$\alpha > \frac{(4s - 2)\sqrt{p} + 4s + 2}{p - 1}. \tag{2.9}$$

Suppose first that Proposition 2.3(i) holds, that is, $k(m) = 4$, $q_{k(m)-1} = 5$ and $m = 9$. Then $q_9 \ge 131$. Also, one can easily see that such a sequence of primes must begin with $q_1 = 2$, $q_2 = 3$ and $q_3 = 5$. Let $s = 2 \cdot 3 \cdot 5$ and $t = q_4 q_5 \cdots q_9$. Then

$$\begin{aligned} 2\frac{\phi(t)}{t} - 1 &\ge 2\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{19}\right)\left(1 - \frac{1}{131}\right) - 1 \\ &\ge 0.27287. \end{aligned}$$

Thus p satisfies (2.9) with $\alpha = 0.27287$ and $s = 30$ if and only if $p > 187899$. Suppose now that there is a prime $p \le 187899$ that satisfies the conditions of the case under analysis. We know that $2 \cdot 3 \cdot 5 \cdot q_9$ divides $p - 1$ with $q_9 \ge 131$. However this requires $q_4 q_5 q_6 q_7 q_8 <$

$187899/(2 \cdot 3 \cdot 5 \cdot 131) \leq 48$ which is clearly not possible, since $q_4 q_5 q_6 q_7 q_8 \geq 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 323323$.

We now consider the other three cases of Proposition 2.3, that is, suppose that Proposition 2.3(ii), (iii) or (iv) holds. In all three cases $k(m) \leq 3$. By assumption $q_1 = 2$, and we now consider the various possibilities for q_2. First, assume that $q_2 = 3$ (note that this is possible in the last two cases) and therefore $m \leq 7$. We set $s = 2 \cdot 3$ and $t = q_3 q_4 q_5 q_6 q_7$. Thus

$$2\frac{\phi(t)}{t} - 1 \geq 2\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{131}\right) - 1 \geq 0.14206.$$

Now p satisfies (2.9) with $\alpha = 0.14206$ and $s = 6$ if and only if $p \geq 24351$. If $p < 24351$ we see that $q_3 q_4 \cdots q_{m-1} < 24351/(2 \cdot 3 \cdot 131) < 31$. Since $q_i \geq 5$ for $i \in \{3, 4, \ldots, m-1\}$ one can see that either $m = 3$ or $m = 4$. In other words, either $t = q_3$ or $t = q_3 q_4$, and thus we can improve the value for α with

$$2\frac{\phi(t)}{t} - 1 \geq 2\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{131}\right) - 1 \geq 0.58778.$$

In this case p satisfies (2.9) with $\alpha = 0.58778$ if and only if $p > 1490$. If $p \leq 1490$ observe that the assumption that $6q_m$ divides $p - 1$ with $q_m \geq 131$ implies that $q_3 < 2$, a contradiction.

We now use the same approach for the case $q_2 = 5$. We choose $s = 2 \cdot 5$ and $t = q_3 q_4 \cdots q_m$. Here we have

$$2\frac{\phi(t)}{t} - 1 \geq 2\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{131}\right) - 1 \geq 0.34361.$$

Hence p satisfies (2.9) with $\alpha = 0.34361$ if and only if $p > 12475$. If, however, $p \leq 12475$ then since $10q_m$ divides $p - 1$ we have that $q_3 < 10$, and so either $m = 3$ or $m = 4$ and $q_3 = 7$. In both cases we can improve the value for α since $t = q_2 q_3$ or $t = q_3 q_4$. In particular,

$$2\frac{\phi(t)}{t} - 1 \geq 2\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{131}\right) - 1 \geq 0.70119956.$$

In this case p satisfies (2.9) with $\alpha = 0.70119956$ if and only if $p > 3057$. If $p \leq 3057$ observe that the assumption that $10q_m$ divides $p - 1$ with $q_m \geq 131$ implies that $q_3 < 3$, a contradiction.

Finally we consider the case $q_2 \geq 7$. Then, by Proposition 2.3, we have $k(m) = 2$ and $m \leq 5$. Here we choose $s = 2$ and use the same technique as above to complete the proof. In particular, we have

$$2\frac{\phi(t)}{t} - 1 \geq 2\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{131}\right) - 1 \geq 0.42758.$$

In this case p satisfies (2.9) with $\alpha = 0.42758$ if and only if $p > 243$. If $p \leq 243$ observe that the assumption that $2q_m$ divides $p - 1$ with $q_m \geq 131$ implies that $q_3 < 2$, a contradiction.

In summary we have seen that given any finite sequence of primes with $q_m \geq 131$ we can choose n in such a way that when $s = q_1 q_2 \cdots q_n$ and $t = q_{n+1} q_{n+2} \cdots q_m$ we have

$$\frac{2\phi(t)}{t} > 1 + \frac{(4s - 2)\sqrt{st + 1}}{st} + \frac{4s + 2}{st}, \tag{2.10}$$

completing the proof of Lemma 2.4. □

In order to proceed with the proof of Theorem 1.1 we now need to identify all those sequences $\{2 = q_1, q_2, \ldots, q_m\}$ with $q_m < 131$ for which one cannot choose $s = q_1 q_2 \cdots q_n$ and $t = q_{n+1} q_{n+2} \cdots q_m$ so as to satisfy (2.10). Since Lemma 2.2 holds for each q_m we can assume that for each of these sequences Proposition 2.3 applies. A computer search of these finitely many sequences yields the exceptional sequences which are listed in Tables 1 and 2. For each of these exceptional sequences we fix $s = q_1 q_2 \cdots q_n$ and $t = q_{n+1} q_{n+2} \cdots q_m$, and we then search for a constant k such that $x > k$ implies the inequality

$$\frac{2\phi(t)}{t} > 1 + \frac{2(2s-1)\sqrt{x}}{x-1} + \frac{4s+2}{x-1}. \tag{2.11}$$

For each of these sequences Tables 1 and 2 give the smallest bound k obtained in this way. The third column of these tables indicates for which choice of t the given bound k is obtained:

Type 1 means that the bound k was obtained with $t = q_{m-1} q_m$,

Type 2 means that the bound was obtained with $t = q_m$, and

Type 3 means that the bound was obtained with $t = 1$.

A computer search then identifies those primes that are smaller than or equal to the bound k, as summarized in the proposition below.

Proposition 2.5. *Let $\{2 = q_1, q_2, \ldots, q_m\}$ be a finite sequence of primes satisfying $m \leq 2k(m) + 1$, and let $p - 1 = q_1^{i_1} q_2^{i_2} \cdots q_m^{i_m}$ with $q_m < 131$. If p is not listed in Tables 1 and 2 then there exist s and t such that*

(i) s and t are coprime,

(ii) a prime q divides $p - 1$ if and only if q divides st, and

(iii) $2\phi(t)/t > 1 + (4s - 2)\sqrt{p}/(p - 1) + (4s + 2)/(p - 1)$.

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. It follows by Proposition 2.1 that a polynomial $f(x)$ represents a nonzero square at some primitive root in F if there exist s and t satisfying the following three conditions:

(i) s and t are coprime,

(ii) a prime q divides $p - 1$ if and only if q divides st, and

(iii) $2\phi(t)/t > 1 + (4s - 2)\sqrt{p}/(p - 1) + (4s + 2)/(p - 1)$.

Our goal is therefore to show that such s and t exist for all odd primes p that are not listed in Tables 1 and 2.

Let $\{q_1 = 2, q_2, \ldots, q_m\}$ be an increasing sequence of prime divisors of $p - 1$. If $m \leq 2k(m) + 1$ then Lemma 2.4 applies for $q_m \geq 131$, and Proposition 2.5 applies for $q_m < 131$.

Table 1: The list of sequences not satisfying (2.10), part I.

Sequence $\mathcal{T}$	k	Type	$p \leq k$ with $\mathcal{T}$	$p \equiv 1 \pmod 4) \leq k$ with $\mathcal{T}$, $(p+1)/2$ prime
2	55	3	$3, 5, 17$	5
$2, 3, 5, 11$	2458	1	$331, 661, 991, 1321$	$661, 1321$
$2, 3, 5, 43$	1622	1	1291	no
$2, 3, 7, 17$	1372	1	no	no
$2, 3, 5, 7, 13$	7040	$t = 455$	2731	no
$2, 3, 43$	460	1	no	no
$2, 3, 31$	496	1	373	no
$2, 3, 61$	435	1	367	no
$2, 3, 5, 7, 23$	5145	$t = 805$	4831	no
$2, 3, 23$	547	1	$139, 277$	277
$2, 3, 67$	430	1	no	no
$2, 3, 7, 13$	1517	1	$547, 1093$	1093
$2, 3, 17$	632	1	$103, 307, 409, 613$	613
$2, 3, 5, 13$	2238	1	$1171, 1951$	no
$2, 3, 11$	788	2	$67, 199, 397, 727$	397
$2, 7$	99	2	29	no
$2, 3, 13$	739	2	$79, 157, 313$	$157, 313$
$2, 3, 7$	1023	2	$43, 127, 337, 379,$ $673, 757, 883, 1009$	$673, 757$
$2, 23$	65	2	47	no
$2, 3, 5, 37$	1656	1	no	no
$2, 5$	133	2	$11, 41, 101$	no
$2, 3, 5, 41$	1632	1	1231	no
$2, 3, 59$	437	1	no	no
$2, 3, 53$	444	1	no	no
$2, 3, 7, 19$	1327	1	no	no
$2, 3, 5, 29$	1727	1	no	no
$2, 17$	69	2	no	no
$2, 11$	78	2	23	no
$2, 3, 5, 19$	1921	1	571	no
$2, 3, 41$	464	1	no	no

Suppose now that $m \geq 2k(m) + 2$. Then, by Lemma 2.2, we have

$$d(k(m)+1, m) > 1 + c_4(k(m)+1, m).$$

If we let $s = q_1 q_2 \cdots q_{k(m)}$ and $t = q_{k(m)+1} \cdots q_m$ we have $2\phi(t)/t = d(k(m)+1, m)$,

Table 2: The list of sequences not satisfying (2.10), part II.

Sequence $\mathcal{T}$	k	Type	$p \leq k$ with $\mathcal{T}$	$p \equiv 1 \pmod 4) \leq k$ with $\mathcal{T}$, $(p+1)/2$ prime
$2, 3, 5, 7, 11$	8160	$t = 385$	$2311, 4621$	4621
$2, 3, 5$	1432	2	$31, 61, 151, 181,$ $241, 271, 541, 601,$ $751, 811, 1201$	$61, 541, 1201$
$2, 3, 5, 47$	1604	1	no	no
$2, 3, 5, 31$	1705	1	no	no
$2, 3, 7, 23$	1265	1	967	no
$2, 5, 17$	180	1	no	no
$2, 3, 11, 13$	1130	1	859	no
$2, 13$	74	2	53	no
$2, 5, 11$	218	1	no	no
$2, 5, 13$	200	1	131	no
$2, 3, 37$	475	1	223	no
$2, 3, 5, 7$	3649	1	$211, 421, 631, 1051,$ $1471, 2521, 3361$	421
$2, 3, 5, 7, 19$	5580	$t = 665$	no	no
$2, 3$	384	2	$7, 13, 19, 37, 73,$ $97, 109, 163, 193$	$13, 37, 73, 193$
$2, 5, 7$	315	1	$71, 281$	no
$2, 3, 5, 23$	1819	1	$691, 1381$	1381
$2, 3, 47$	453	1	283	no
$2, 3, 5, 7, 17$	5905	$t = 595$	3571	no
$2, 3, 29$	506	1	349	no
$2, 3, 7, 11$	1646	1	463	no
$2, 3, 5, 17$	1995	1	$1021, 1531$	no
$2, 29$	63	2	59	no
$2, 3, 19$	596	1	$229, 457$	457
$2, 19$	68	2	no	no

and

$$
\begin{aligned}
c_4(k(m)+1, m) &= 8 \cdot \sqrt{\frac{q_1 q_2 \cdots q_{k(m)}}{q_{k(m)+1} q_{k(m)+2} \cdots q_m}} \\
&= \frac{8s}{\sqrt{q_1 q_2 \cdots q_m}} \geq \frac{8s}{\sqrt{p-1}}
\end{aligned}
$$

Since s is even and $4(p-1) \geq 4s \geq 3$ we may apply [9, Lemma 6] to see that

$$
\frac{(4s-2)\sqrt{p}}{p-1} \leq \frac{4s}{\sqrt{p-1}}.
$$

It follows that

$$\begin{aligned}\frac{2\phi(t)}{t} &= d(k(m)+1,m) \geq 1 + c_4(k(m)+1,m) \geq 1 + \frac{8s}{\sqrt{p-1}}\\ &\geq 1 + \frac{(4s-2)\sqrt{p}}{p-1} + \frac{4s+2}{p-1}.\end{aligned}$$

(Note that the last inequality holds since $p \geq 7$.) □

For the sake of completeness we would like to add the following proposition (obtained with a computer search) which deals with exceptional primes p not covered by Theorem 1.1 which are congruent to 1 modulo 4 and for which $(p+1)/2$ is also a prime (primes given in the last column of Tables 1 and 2). As is the case with Theorem 1.1 this proposition too is used in the construction of Hamilton cycles in vertex-transitive graphs of order a product of two primes in [5].

Proposition 2.6. *Let F be a finite field of odd prime order p, and let $k \in F$. If*

$$\begin{aligned}p \in \{&5, 13, 37, 61, 73, 157, 193, 277, 313, 397, 421, 457, 541,\\ &613, 661, 673, 757, 1093, 1201, 1321, 1381, 4621\}\end{aligned}$$

then there exists a primitive root β of F such that $f(\beta) = \beta^4 + k\beta^2 + 1$ is a square in F except when

$$\begin{aligned}(p,k) \in \{&(5,4), (13,1), (13,4), (13,5), (13,6), (13,7), (13,10),\\ &(37,3), (37,28), (37,29), (61,18), (61,37), (61,40)\}.\end{aligned}$$

Amongst these exceptions only for $(p,k) \in \{(13,1), (37,28), (61,18)\}$ there exists $\xi \in S^* \cap (S^*+1)$ such that $k = 2(1-2\xi)$. In particular, $\xi = 10$ for $(p,k) = (13,1)$, $\xi = 12$ for $(p,k) = (37,28)$, and $\xi = 57$ for $(p,k) = (61,18)$. Moreover, amongst these exceptions only for $(p,k) \in \{(13,1), (37,28), (61,18)\}$ there exists $\bar{\xi} \in S^* \cap (S^*+1)$ such that $k = -2(1-2\bar{\xi})$. In particular, $\bar{\xi} = 4$ for $(p,k) = (13,1)$, $\bar{\xi} = 26$ for $(p,k) = (37,28)$, and $\bar{\xi} = 5$ for $(p,k) = (61,18)$.

References

[1] B. Alspach, Lifting Hamilton cycles of quotient graphs, *Discrete Math.* **78** (1989), 25–36, doi:10.1016/0012-365x(89)90157-x.

[2] B. Alspach, K. Heinrich and M. Rosenfeld, Edge partitions of the complete symmetric directed graph and related designs, *Israel J. Math.* **40** (1981), 118–128, doi:10.1007/bf02761904.

[3] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič and L. A. Nowitz, Transitive permutation groups without semiregular subgroups, *J. London Math. Soc.* **66** (2002), 325–333, doi:10.1112/s0024610702003484.

[4] P. J. Cameron (ed.), Research problems from the Fifteenth British Combinatorial Conference, *Discrete Math.* **167/168** (1997), 605–615, doi:10.1016/s0012-365x(96)00212-9.

[5] S. F. Du, K. Kutnar and D. Marušič, Hamilton cycles in vertex-transitive graphs of order a product of two primes, arXiv:1808.08553 [math.CO].

[6] Y.-Q. Feng, D.-W. Yang and J.-X. Zhou, Arc-transitive cyclic and dihedral covers of pentavalent symmetric graphs of order twice a prime, *Ars Math. Contemp.* **15** (2018), 499–522, doi:10.26493/1855-3974.1409.e54.

[7] K. Kutnar and D. Marušič, Hamilton cycles and paths in vertex-transitive graphs—current directions, *Discrete Math.* **309** (2009), 5491–5500, doi:10.1016/j.disc.2009.02.017.

[8] L. Lovász, The factorization of graphs, in: R. Guy, H. Hanam, N. Sauer and J. Schonheim (eds.), *Combinatorial Structures and Their Applications*, Gordon and Breach, New York, 1970 pp. 243–246, proceedings of the Calgary International Conference on Combinatorial Structures and their Applications held at the University of Calgary, Calgary, Alberta, Canada, June 1969.

[9] D. J. Madden and W. Y. Vélez, Polynomials that represent quadratic residues at primitive roots, *Pacific J. Math.* **98** (1982), 123–137, `http://projecteuclid.org/euclid.pjm/1102734391`.

[10] D. Marušič, On vertex symmetric digraphs, *Discrete Math.* **36** (1981), 69–81, doi:10.1016/0012-365x(81)90174-6.

[11] D. Marušič, Hamiltonian circuits in Cayley graphs, *Discrete Math.* **46** (1983), 49–54, doi:10.1016/0012-365x(83)90269-8.

[12] D. Marušič, Semiregular automorphisms in vertex-transitive graphs with a solvable group of automorphisms, *Ars Math. Contemp.* **13** (2017), 461–468, doi:10.26493/1855-3974.1486.a33.

[13] G. Verret, Arc-transitive graphs of valency 8 have a semiregular automorphism, *Ars Math. Contemp.* **8** (2015), 29–34, doi:10.26493/1855-3974.492.37d.

[14] Y. Wang and Y.-Q. Feng, Half-arc-transitive graphs of prime-cube order of small valencies, *Ars Math. Contemp.* **13** (2017), 343–353, doi:10.26493/1855-3974.964.594.