ON EXPLICIT FACTORS OF CYCLOTOMIC POLYNOMIALS OVER FINITE FIELDS

LIPING WANG AND QIANG WANG

ABSTRACT. We study the explicit factorization of $2^n r$-th cyclotomic polynomials over finite field $\mathbb{F}_q$ where q, r are odd with $(r, q) = 1$. We show that all irreducible factors of $2^n r$-th cyclotomic polynomials can be obtained easily from irreducible factors of cyclotomic polynomials of small orders. In particular, we obtain the explicit factorization of $2^n 5$-th cyclotomic polynomials over finite fields and construct several classes of irreducible polynomials of degree 2^{n-2} with fewer than 5 terms.

1. INTRODUCTION

Let p be prime, $q = p^m$, and $\mathbb{F}_q$ be a finite field of order q. Let $Q_n(x)$ denote the n-th cyclotomic polynomial

$$Q_n(x) = \prod_{0<j\le n,(j,n)=1} (x - \zeta^j),$$

where ζ is a primitive n-th root of unity. Clearly $x^n - 1 = \prod_{d|n} Q_d(x)$ and the Möbius inversion formula gives $Q_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$ where μ is the Möbius function. If $(q, n) = 1$, then it is well known that $Q_n(x)$ can be factorized into $\phi(n)/d$ distinct monic irreducible polynomials of the same degree d over $\mathbb{F}_q$, where d is the least positive integer such that $q^d \equiv 1 \pmod{n}$ (see [8, Theorem 2.47]). Basically we know the number and the degree of irreducible factors of cyclotomic polynomials. However, factoring cyclotomic polynomials $Q_n(x)$ over the finite field $\mathbb{F}_q$ explicitly still remains a fundamental question. Moreover, it is also known that explicit factorization of cyclotomic polynomials is related to the factorization of other interesting classes of polynomials. For example, Fitzgerald and Yucas [4] recently discovered a nice link between the factors of Dickson polynomials over finite fields and factors of cyclotomic polynomials and self-reciprocal polynomials. This means that factoring cyclotomic polynomials explicitly provides an alternative way to factor Dickson polynomials explicitly.

Explicit factorization of 2^n-th cyclotomic polynomials $Q_{2^n}(x)$ over $\mathbb{F}_q$ is given in [8] when $q \equiv 1 \pmod 4$ and in [9] when $q \equiv 3 \pmod 4$. Recently, Fitzgerald and Yucas [5] have studied explicit factors of $Q_{2^n r}(x)$, where r is prime and $q \equiv \pm 1 \pmod r$ over finite field $\mathbb{F}_q$ in order to obtain explicit factorization of Dickson polynomials. This gives a complete answer to the explicit factorization of cyclotomic polynomials $Q_{2^n 3}(x)$ and thus Dickson polynomials $D_{2^n 3}(x)$ of the first kind over $\mathbb{F}_q$. However, the general situation for arbitrary r remains open. Without loss of generality we assume that $(2r, q) = 1$. In this paper, we reduce the problem of factorizing all $2^n r$-th cyclotomic polynomials over $\mathbb{F}_q$ into factorizing a finite number of lower degree cyclotomic polynomials over $\mathbb{F}_q$. In particular, we give the explicit factorization of $Q_{2^n r}(x)$ over $\mathbb{F}_q$ where $r = 5$. The method we are using is a combination of case by case analysis, factorizing low degree polynomials, and the recursive construction based on basic properties of cyclotomic polynomials.

2000 *Mathematics Subject Classification.* 11T06, 11T55, 12Y05.

Key words and phrases. factorization, cyclotomic polynomials, irreducible polynomials, Dickson polynomials, finite fields.

Research is partially supported by National Natural Science Foundation of China (Grant No. 60773141 and No.10990011) and NSERC of Canada.

The irreducible factors of these cyclotomic polynomials are sparse polynomials (polynomials with a few nonzero terms). Sparse irreducible polynomials are important in efficient hardware implementation of feedback shift registers and finite field arithmetic ([1], [7], [10]). The second focus of our paper is to explicitly construct sparse irreducible polynomials of high degree. We remark that explicit construction of irreducible polynomials in general has attracted a lot of attention and a lot of progress has made in the past two decades. Most of these constructions are iterated constructions which extend the classical transformation $f(x) \to f(x^n)$. A a nice survey on this topic as of year 2005 can be found in [3]. Here we are interested in sparse irreducible polynomials and the classical transformation is used. Therefore the main tool in the paper is the following classical result which helps us to construct high degree irreducible polynomials based on low degree irreducible polynomials.

Lemma 1.1 (Theorem 3.35 in [8])**.** *Let $f_1(x)$, $f_2(x)$, ..., $f_N(x)$ be all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m and order e, and let $t \geq 2$ be an integer whose prime factors divide e but not $(q^m-1)/e$. Assume also that $q^m \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$. Then $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ are all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et.*

In Section 2, we describe the methodology used in this paper to factor $Q_{2^n r}(x)$ over $\mathbb{F}_q$. We prove that all irreducible factors of $Q_{2^n r}(x)$ can be obtained easily from irreducible factors of $Q_{2^L r}(x)$ where L is a small constant depending on q and r (Theorem 2.2). This also gives a way to construct sparse irreducible polynomials of high degree $2^n r$ over $\mathbb{F}_q$. We note that the result in this section is true for any odd q, r such that $(q, r) = 1$. Then the rest of paper deals with $r = 5$. In Section 3, we obtained the factorization results of $Q_{2^n 5}(x)$ when $q \equiv \pm 1 \pmod 5$. Since our results (Theorems 3.2, 3.4, 3.5) for middle term are substantial simplification of the corresponding results in [5], we include proofs for the sake of completeness. Moreover, we obtain several classes of irreducible binomials/trinomials of degree 2^{n-2} over $\mathbb{F}_q$ where $q \equiv \pm 1 \pmod 5$. We note that our explicit factorization results are given in terms of 2^n-th primitive roots of unity and it may cause additional task to compute these roots. However, we also could reformulate these results in terms of solving system of nonlinear recurrence relations, which seems pretty fast when providing examples for small fields. In Section 4, we consider the situation when $q \equiv 13, 17 \pmod{20}$. We obtain the explicit factorization of $Q_{2^n 5}(x)$ in Theorems 4.1. Moreover, we can construct several classes of irreducible polynomial of five terms with degree 2^m (Corollary 4.2). Then the cases of $q \equiv 3, 7 \pmod{20}$ are considered in Section 5. In Theorem 5.1 we show that coefficients of the irreducible factors of $2^n 5$-th cyclotomic polynomials are obtained from the coefficients of irreducible factors of $2^{n-1}5$-th cyclotomic polynomials by solving some simple systems of nonlinear recurrence relations for $n \leq L$. Similarly we construct a class of irreducible polynomials over these fields (Corollary 5.2). We note that it is very fast to solve these systems of nonlinear recurrence relations and to obtain the factors of cyclotomic polynomials. As an illustration, we provide two tables of examples in Section 5.

We note that the sparse irreducible polynomials constructed in this paper and their reciprocal polynomials can both be written in the form of $x^n + g(x)$, where the degree of $g(x)$ is at most $3n/4$. It is well known that irreducible polynomials of the form $x^n + g(x)$ with $g(x)$ of small degree are desirable in implementing pseudo-random number generators and in constructing elements of provable high orders in finite fields (see the survey paper [6]). We wonder whether or not irreducible polynomials constructed in this paper could be useful in some of applications mentioned in [6].

2. Methodology and notations

In this section, we describe the method that we are using in this paper. First of all we recall the following basic results on cyclotomic polynomials.

Lemma 2.1. [8, Exercise 2.57]
(a) $Q_{2n}(x) = Q_n(-x)$ for $n \geq 3$ and n odd.
(b) $Q_{mt}(x) = Q_m(x^t)$ for all positive integers m that are divisible by the prime t.

(c) $Q_{mt^k}(x) = Q_{mt}(x^{t^{k-1}})$ *if* t *is a prime and* m, k *are arbitrary positive integers.*

Let us start with the factorizations of $Q_r(x)$ and $Q_{2r}(x) = Q_r(-x)$. Applying Lemma 2.1, we have $Q_{2^n r}(x) = Q_{2^{n-1}r}(x^2)$ for $n \geq 2$. Hence the key to continue the process of factorization is to factor $Q_{2^{n-1}r}(x^2)$ into a product of irreducible polynomials once we obtain the factorization of $Q_{2^{n-1}r}(x)$.

Now, we show that we can reach to the end after only a finite number of iterations. Let $v_2(k)$ denotes the highest power of 2 dividing k and $L_i = v_2(q^i - 1)$ for $i \geq 1$. In particular, let $L := L_{\phi(r)} = v_2(q^{\phi(r)} - 1)$ where ϕ is the Euler's phi function. Then we have the following result.

Theorem 2.2. *Let* $q = p^m$ *be a power of an odd prime* p*, let* $r \geq 3$ *be any odd number such that* $(r, q) = 1$*, and let* $L := L_{\phi(r)} = v_2(q^{\phi(r)} - 1)$*, the highest power of* 2 *dividing* $q^{\phi(r)} - 1$ *with* $\phi(r)$ *the Euler's phi function. For any* $n \geq L$ *and any irreducible factor* $f(x)$ *of* $Q_{2^L r}(x)$ *over* $\mathbb{F}_q$*,* $f(x^{2^{n-L}})$ *is also irreducible over* $\mathbb{F}_q$*. Moreover, all irreducible factors of* $Q_{2^n r}(x)$ *are obtained in this way.*

Proof. Since q, r are odd, we have $\phi(r)$ is even and then $n \geq L \geq 2$. By [8, Theorem 2.47], $2^L r$-th cyclotomic polynomial $Q_{2^L r}(x)$ has $\phi(2^L r)/m$ distinct monic irreducible factors of the same degree m, where m is the least positive integer such that $q^m \equiv 1 \pmod{2^L r}$. Due to the fact that $q^{\phi(r)} \equiv 1 \pmod{r}$ and $L = v_2(q^{\phi(r)} - 1)$, we have $q^{\phi(r)} \equiv 1 \pmod{2^L r}$. This implies that $m \leq \phi(r)$. By the definition of L, we must have $2^{L+1} \nmid (q^m - 1)$. Since each factor has order $e = 2^L r$ and $2 \nmid (q^m - 1)/e$, by Lemma 1.1, each irreducible polynomial $f(x)$ of $Q_{2^L r}(x)$ generates an irreducible factor $f(x^2)$ of $Q_{2^{L+1}r}(x)$. More generally, $f(x^{2^{n-L}})$ is also irreducible factor of $Q_{2^n r}(x)$ since $L \geq 2$ implies that $4 \mid q^m - 1$. Moreover, $f(x^{2^{n-L}})$ has degree $m2^{(n-L)}$ and order $2^n r$. Hence there are $\phi(2^n r)/(m2^{n-L}) = 2^{n-1}\phi(r)/(m2^{n-L}) = \phi(2^L r)/m$ distinct irreducible factors for $Q_{2^n r}(x)$. Therefore all irreducible factors of $Q_{2^n r}(x)$ are constructed from irreducible factors of $Q_{2^L r}(x)$ over $\mathbb{F}_q$. □

We remark that there exists a simple formula for $v_2(q^i - 1)$. For odd q, by Proposition 1 in [2], we have

$$(1)\quad v_2(q^i - 1) = v_2(q-1) + v_2(q^{i-1} + q^{i-2} + \ldots + 1) = \begin{cases} v_2(q-1) + v_2(i) + v_2(q+1) - 1, & \text{if } i \text{ is even;} \\ v_2(q-1), & \text{if } i \text{ is odd.} \end{cases}$$

Since r is odd, we must have $\phi(r)$ is even. In particular, we have $v_2(q^{\phi(r)} - 1) = v_2(q-1) + v_2(\phi(r)) + v_2(q+1) - 1$.

Theorem 2.2 tells us that a recursive way of factoring $2^n r$-th cyclotomic polynomials essentially requires only finitely many factorizations of low degree polynomials (at most L iterations starting from $Q_r(x)$). This also gives a way to construct irreducible polynomials from low degree irreducible polynomials. The fact that we use the classical transformation on low degree polynomials can guarantee the resulting high degree irreducible polynomials are sparse polynomials.

For $n < L$, since each irreducible factor $f(x)$ of $Q_{2^{n-1}r}(x)$ has the same degree m and $f(x^2)$ may not be irreducible polynomial of degree $2m$, we need to factor $f(x^2)$ further. And in most cases, we need to factor $f(x^2)$ into two irreducible polynomials of degree m. We see more in detail for $r = 5$ in the forthcoming sections. This involves the process of factoring certain types of polynomials of degree 8 into two quartic polynomials.

Finally we fix some other notations for the rest of the paper.

Let $\Omega(k)$ denote the set of primitive k-th root of unity. In particular, $\Omega(2^0) = \{1\}$, $\Omega(2^1) = \{-1\}$. Let ρ_n denote an arbitrary element in $\Omega(2^n)$.

The expression $\prod_{a \in A} \cdots \prod_{b \in B} f_i(x, a, \ldots, b)$ denotes the product of *distinct* irreducible polynomials $f_i(x, a, \ldots, b)$ satisfying conditions $a \in A$, …, $b \in B$. For example, in the expression

$$\prod_{w \in \Omega(5)} \prod_{\rho_n \in \Omega(2^n)} \left(x^2 - (\rho_n + \rho_n^{-1})wx + w^2\right),$$

we only take distinct factors because both ρ_n and ρ_n^{-1} yield the same coefficient $(\rho_n + \rho_n^{-1})w$.

Let $\left(\frac{a}{p}\right)$ denote the Legendre symbol and the following basic results on Legendre symbols are also used in the paper.

(i) $\left(\frac{2}{p}\right)=1$ if and only if $p\equiv 1,7 \pmod 8$;

(ii) $\left(\frac{-2}{p}\right)=1$ if and only if $p\equiv 1,3 \pmod 8$;

(iii) $\left(\frac{5}{p}\right)=1$ if and only if $p\equiv \pm 1,\pm 9 \pmod{20}$.

3. The case $q\equiv \pm 1 \pmod 5$

Recall that $L_i=v_2(q^i-1)$, the highest power of 2 dividing q^i-1 for $i\geq 1$. If $q\equiv \pm 1 \pmod 5$ and $q\equiv 1 \pmod 4$ (i.e., $q=20k+1$ or $q=20k+9$), then $L_4=L_2+1$, $L_2=L_1+1$, and $L_1=4+v_2(5k)$ or $L_1=2+v_2(5k+2)$, respectively. Moreover, $\rho_1=-1$ must be a square and thus $\rho_2^2=\rho_1$.

Similarly, if $q\equiv \pm 1 \pmod 5$ and $q\equiv 3 \pmod 4$ (i.e., $q=20k+11$ or $q=20k+19$), then $L_4=L_2+1$, $L_1=1$, $L_2=3+v_2(5k+3)$ or $L_2=3+v_2(5k+5)$, respectively. Moreover, $\rho_1=-1$ can not be a square.

We have the following results for these four different cases. The first result is the same as in [5], so we omit the proof.

Theorem 3.1. *Let $q\equiv 1 \pmod{20}$. Then we have the following factorization of $Q_{2^n5}(x)$ over $\mathbb{F}_q$.*

(i) $Q_5(x)=\prod_{w\in\Omega(5)}(x-w)$ and $Q_{10}(x)=\prod_{w\in\Omega(5)}(x+w)$.

(ii) If $2\leq n\leq L_1$, then

$$Q_{2^n5}(x)=\prod_{w\in\Omega(5)}\prod_{\rho_n\in\Omega(2^n)}(x-w\rho_n).$$

(iii)if $n\geq L_2=L_1+1$, then

$$Q_{2^n5}(x)=\prod_{w\in\Omega(5)}\prod_{\rho_{L_1}\in\Omega(2^{L_1})}\left(x^{2^{n-L_1}}-w\rho_{L_1}\right).$$

Theorem 3.2. *Let $q=20k+11$ for some non-negative integer k. Then we have the following factorization of $Q_{2^n5}(x)$ over $\mathbb{F}_q$.*

(i) For $n=0,1,2$, we have

$$Q_5(x)=\prod_{w\in\Omega(5)}(x-w),\ Q_{10}(x)=\prod_{w\in\Omega(5)}(x+w),\ Q_{20}(x)=\prod_{w\in\Omega(5)}\left(x^2+w\right).$$

(ii) if $3\leq n<L_2$, then

$$Q_{2^n5}(x)=\prod_{w\in\Omega(5)}\prod_{\rho_n\in\Omega(2^n)}\left(x^2-(\rho_n+\rho_n^{-1})wx+w^2\right).$$

(iii) if $n\geq L_2$, then

$$Q_{2^n5}(x)=\prod_{w\in\Omega(5)}\prod_{\rho_{L_2}\in\Omega(2^{L_2})}\left(x^{2^{n-L_2+1}}-(\rho_{L_2}-\rho_{L_2}^{-1})wx^{2^{n-L_2}}-w^2\right).$$

In particular, if k is even then $L_2=3$ and for any $n\geq 3$,

$$Q_{2^n5}(x)=\prod_{w\in\Omega(5)}\prod_{c^2=-2}\left(x^{2^{n-2}}+cwx^{2^{n-3}}-w^2\right).$$

Proof. In this case, $L_1=v_2(q-1)=1$, $L_2=v_2(q^2-1)=3+v_2(5k+3)$, and $L_4=L_2+1$. We note that $L_2=3$ if n is even. It is obvious that $Q_5(x)=\prod_{w\in\Omega(5)}(x-w)$, and $Q_{10}(x)=Q_5(-x)=\prod_{w\in\Omega(5)}(x+w)$ because $5\mid q-1$. Moreover, -1 is a non-square in $\mathbb{F}_q$ when $q\equiv 3 \pmod 4$. Hence x^2+w is irreducible in $\mathbb{F}_q[x]$ and then $Q_{20}(x)=Q_{10}(x^2)=\prod_{w\in\Omega(5)}\left(x^2+w\right)$. Now $Q_{40}(x)=Q_{20}(x^2)=\prod_{w\in\Omega(5)}\left(x^4+w\right)$.

Since $\gcd(40, q) = 1$ and $q^2 \equiv 1 \pmod{40}$, by Theorem 2.47 in [8], $Q_{40}(x)$ factors into $\phi(40)/2 = 8$ distinct monic quadratic irreducible polynomials in $\mathbb{F}_q[x]$. Hence $x^4 + w$ can be factorized into a product of two monic quadratic polynomials. Let $x^4 + w = (x^2 + ax + b)(x^2 + cx + d)$ where $a, b, c, d \in \mathbb{F}_q$. Comparing both sides, we have $a + c = 0$, $b + d + ac = 0$, $bd + ad = 0$, and $bd = w$. Replacing a by $-c$, we obtain $b + d - c^2 = 0$, $(b - d)c = 0$, and $bd = w$. Here we can write $w = v^4$ where $v = w^{-1}$ because $w^5 = 1$. Using the fact that -1 is a non-square in this case, we can only have two possible solutions ($c \neq 0$ because, otherwise, $b^2 = -v^4$, a contradiction): (i) $b = d = v^2$, $a = -c$, and $c^2 = 2v^2$ if 2 is a square; (ii) $b = d = -v^2$, $a = -c$, and $c^2 = -2v^2$ if -2 is a square. We note that $q \equiv 4k + 3 \pmod 8$. Hence if k is even, then $q \equiv 3 \pmod 8$; otherwise, $q \equiv 7 \pmod 8$. Moreover, $q \equiv 3 \pmod 8$ implies that the characteristic p of $\mathbb{F}_q$ also satisfies $p \equiv 3 \pmod 8$, therefore -2 is a square in $\mathbb{F}_q$ if k is even. Similarly, 2 is a square in $\mathbb{F}_q$ if k is odd. As w ranges over $\Omega(5)$, v also ranges over $\Omega(5)$. Hence we obtain

$$Q_{40}(x) = \begin{cases} \displaystyle\prod_{w\in\Omega(5)} \prod_{c^2=-2} \left(x^2 + cwx - w^2\right), & if \text{ k } is\ even; \\ \displaystyle\prod_{w\in\Omega(5)} \prod_{c^2=2} \left(x^2 + cwx + w^2\right), & if \text{ k } is\ odd; \end{cases}$$

If k is even, then $L_2 = 3$ and $2^{n-2} \nmid (q^2 - 1)/40$ for $n \geq 3$. Moreover, each $x^2 + cwx - w^2$ with $c^2 = -2$ is an irreducible polynomial of degree 2 and order 40. If $n \geq 4$, then $2^{n-2} \equiv 0 \pmod 4$ and $q^2 - 1 \equiv 0 \pmod 4$. Hence by Lemma 1.1, we have that $x^{2^{n-2}} + cwx^{2^{n-3}} - w^2$ is irreducible and

$$Q_{2^n 5}(x) = Q_{2^3 5}(x^{2^{n-3}}) = \prod_{w\in\Omega(5)} \prod_{c^2=-2} \left(x^{2^{n-2}} + cwx^{2^{n-3}} - w^2\right).$$

In particular, $\rho_3 - \rho_3^{-1} = \rho_3 + \rho_3^q \in \mathbb{F}_q$ and $(\rho_3 - \rho_3^{-1})^2 = -2$.

If k is odd, then $L_2 > 3$. For each n such that $3 \leq n < L_2$, we have $\rho_n^{q+1} = 1$ for any $\rho_n \in \Omega(2^n)$. Hence $\rho_n + \rho_n^{-1} = \rho_n + \rho_n^q \in \mathbb{F}_q$ for $3 \leq n < L_2$. In particular, $\rho_2 + \rho_2^{-1} = 0$ and $\left(\pm(\rho_3 + \rho_3^{-1})\right)^2 = 2$. Therefore

$$Q_{40}(x) = \prod_{w\in\Omega(5)} \prod_{\rho_3\in\Omega(2^3)} \left(x^2 - (\rho_3 + \rho_3^{-1})wx + w^2\right).$$

Let $w = u^2$. Then for each $3 \leq n < L_2$, we have

$$\left(x^4 - (\rho_{n-1} + \rho_{n-1}^{-1})u^2x^2 + u^4\right) = \left(x^2 - (\rho_n + \rho_n^{-1})ux + u^2\right)\left(x^2 + (\rho_n + \rho_n^{-1})ux + u^2\right).$$

Hence, for odd k and $3 \leq n < L_2$, we obtain

$$Q_{2^n 5}(x) = \prod_{w\in\Omega(5)} \prod_{\rho_n\in\Omega(2^n)} \left(x^2 - (\rho_n + \rho_n^{-1})wx + w^2\right).$$

We note that in the above expression we only take distinct irreducible factors.

Finally, for odd k and $n \geq L_2$, it is easy to see that $\rho_{L_2}^{2(q+1)} = 1$ and $\rho_{L_2}^{q+1} \neq 1$. This implies that $\rho_{L_2}^{q+1} = -1$ and thus $\rho_{L_2} - \rho_{L_2}^{-1} \in \mathbb{F}_q$. Moreover,

$$\left(x^4 - (\rho_{L_2-1} + \rho_{L_2-1}^{-1})u^2x^2 + u^4\right) = \left(x^2 - (\rho_{L_2} - \rho_{L_2}^{-1})ux - u^2\right)\left(x^2 + (\rho_{L_2} - \rho_{L_2}^{-1})ux - u^2\right).$$

Hence

$$Q_{2^{L_2}5}(x) = \prod_{w\in\Omega(5)} \prod_{\rho_{L_2}\in\Omega(2^{L_2})} \left(x^2 - (\rho_{L_2} - \rho_{L_2}^{-1})wx - w^2\right).$$

Since $q^2 \equiv 1 \pmod{2^{L_2}5}$ and $2 \nmid (q^2-1)/2^{L_2}5$, by Lemma 1.1, we conclude that $x^4-(\rho_{L_2}-\rho_{L_2}^{-1})wx^2-w^2$ is irreducible and

$$Q_{2^{L_5}}(x) = Q_{2^{L_2}5}(x^2) = \prod_{w\in\Omega(5)} \prod_{\rho_{L_2}\in\Omega(2^{L_2})} \left(x^4 - (\rho_{L_2}-\rho_{L_2}^{-1})wx^2 - w^2\right).$$

The rest of proof follows directly from Theorem 2.2 and the fact that $L_4 = L_2+1$ in this case. □

It is not difficult to see from the proof that we can also reformulate the above result as follows.

Corollary 3.3. *Let $q \equiv 11 \pmod{20}$. For any $2 \le n \le L_2$, we have*

$$Q_{2^n5}(x) = \prod_{w\in\Omega(5)} \prod_{a_n,b_n} \left(x^2 + a_n x + b_n\right),$$

where a_n, b_n are all the solutions to the system of nonlinear recurrence relations

$$\begin{cases} a_n^2 &= 2b_n - a_{n-1} \\ b_n^2 &= b_{n-1}, \end{cases}$$

with initial values $a_2 = 0$ and $b_2 = w \in \Omega(5)$. For $n > L_2$,

$$Q_{2^n5}(x) = \prod_{w\in\Omega(5)} \prod_{a_{L_2},b_{L_2}} \left(x^{2^{n-L_2+1}} + a_{L_2}x^{2^{n-L_2}} + b_{L_2}\right).$$

Theorem 3.4. *Let $q = 20k+9$, $w \in \Omega(5)$ be fixed, and $L_i = v_2(q^i-1)$ for $i \ge 1$. Then we have the following factorization of $Q_{2^n5}(x)$ over $\mathbb{F}_q$.*

(i) For $n = 0, 1$, we have

$$Q_5(x) = \prod_{j=1,2} \left(x^2 - (w^j + w^{-j})x + 1\right),\ Q_{10}(x) = \prod_{j=1,2} \left(x^2 + (w^j + w^{-j})x + 1\right).$$

(ii) if $2 \le n \le L_1$, then

$$Q_{2^n5}(x) = \prod_{\rho_n\in\Omega(2^n)} \prod_{a_n=\rho_n\prod_{j=1,2}(w^j+w^{-j})} \left(x^2 + a_n x + \rho_n^2\right).$$

(iii) if $n \ge L_2 = L_1+1$, then

$$Q_{2^n5}(x) = \prod_{\rho_{L_1}\in\Omega(2^{L_1})} \prod_{a_{L_2}^2=\rho_{L_1}\prod_{j=1,2}(2-w^j-w^{-j})} \left(x^{2^{n-L_2+1}} + a_{L_2}x^{n-L_2} + \rho_{L_1}\right).$$

In particular, if k is odd then $L_2 = 3$ and for any $n \ge 3$,

$$Q_{2^n5}(x) = \prod_{\rho_2\in\Omega(2^2)} \prod_{a_3^2=\rho_2\prod_{j=1,2}(2-w^j-w^{-j})} \left(x^{2^{n-2}} + a_3x^{n-3} + \rho_2\right).$$

Proof. Let $q = 20k+9$. Then $L_1 = 2+v_2(5k+2)$, $L_2 = L_1+1$, and $L_4 = L_2+1$. In particular, if k is odd, then $L_1 = 2$. As $5 \nmid q-1$, $w \in \Omega(5)$ implies $w \notin \mathbb{F}_q$. However, $5 \mid q+1$ implies $a = w+w^{-1} = w+w^q \in \mathbb{F}_q$. Hence $Q_5(x) = \prod_{j=1,2} \left(x^2 - (w^j + w^{-j})x + 1\right)$, and $Q_{10}(x) = Q_5(-x) = \prod_{j=1,2} \left(x^2 + (w^j + w^{-j})x + 1\right)$.

Let $a_1 = w^j + w^{-j}$ for $j = 1$ or 2. Then $Q_{20}(x) = Q_{10}(x^2) = \prod_{\substack{a_1=w+w^{-1}\\ j=1,2}} \left(x^4 + a_1x^2 + \rho_0\right)$. Again, $q^2 \equiv 1 \pmod{2^{L_1}5}$ and Theorem 2.47 in [8] imply that $Q_{2^n5}(x)$ factors into distinct monic quadratic

polynomials. In order to factor $Q_{20}(x)$, we need to factor $x^4+a_1x^2+\rho_0$ into monic quadratic irreducible polynomials. Let $x^4+a_1x^2+\rho_0=(x^2+bx+c)(x^2+dx+e)$ where $b,c,d,e\in\mathbb{F}_q$. Then we obtain

$$\begin{aligned} b+d &= 0\\ c+e+bd &= a_1\\ be+cd &= 0\\ ce &= \rho_0 \end{aligned}$$

Hence $b=-d$. Continue to solve the above system, either we have $b=-d=0$ or $e=c$. If $b=-d=0$, then c satisfies that $c^2-ac+1=0$, contradicts to that x^2-ax+1 is irreducible. Hence $e=c$. Let $x^4+a_1x^2+\rho_0=(x^2+a_2x+c)(x^2-a_2x+c)$. Therefore $e=c=\pm\rho_1\in\mathbb{F}_q$ and $a_2^2=\pm2\rho_1-a_1$. Since we can verify directly that $a_2=\rho_2(w^{3j}+w^{-3j})\in\mathbb{F}_q$ are solutions to $a_2^2=2\rho_1-a_1$ where $\rho_2^2=\rho_1$, we obtain

$$Q_{20}(x)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2(w^j+w^{-j})\\ j=1,2}}\left(x^2+a_2x+\rho_2^2\right).$$

Now

$$Q_{40}(x)=Q_{20}(x^2)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2(w^j+w^{-j})\\ j=1,2}}\left(x^4+a_2x^2+\rho_2^2\right).$$

If k is odd, then $L_1=2$. Let $\left(x^4+a_2x^2+\rho_2^2\right)=\left(x^2+a_3x+\rho_2\right)\left(x^2-a_3x+\rho_2\right)$ where $a_3,\rho_2\in\mathbb{F}_q$. Hence $a_3^2=2\rho_2-a_2$. Since $2\rho_2-\rho_2(w^j+w^{-j})=-\rho_2(w^{3j}-w^{-3j})^2\in\mathbb{F}_q$ and both ρ_2 and $-(w^{3j}-w^{-3j})^2$ are non-square elements in $\mathbb{F}_q$, there exist $a_3\in\mathbb{F}_q$ such that $a_3^2=2\rho_2-a_2$. Hence

$$Q_{40}(x)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2(w^j+w^{-j})\\ j=1,2}}\prod_{a_3^2=2\rho_2-a_2}\left(x^2+a_3x+\rho_2\right).$$

We note that $L_2=3$ implies $2\nmid(q^2-1)/40$. By Lemma 1.1, $x^4+a_3x^2+\rho_2$ is irreducible and

$$Q_{80}(x)=Q_{40}(x^2)\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2(w^j+w^{-j})\\ j=1,2}}\prod_{a_3^2=2\rho_2-a_2}\left(x^4+a_3x^2+\rho_2\right).$$

Moreover, for any $n>4$, by Theorem 2.2, we conclude $x^{2^{n-2}}+a_3x^{2^{n-3}}+\rho_2$ is irreducible. Hence for odd k and $n\geq3$ we have

$$Q_{2^n5}(x)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_3^2=\rho_2(2-w^j-w^{-j})\\ j=1,2}}\left(x^{2^{n-2}}+a_3x^{n-3}+\rho_2\right).$$

If k is even, then $L_1\geq3$. For any $3\leq n<L_1$, we have $\rho_n\in\mathbb{F}_q$ and $a_n=\rho_n(w^j+w^{-j})\in\mathbb{F}_q$. Let $\rho_{n-1}=\rho_n^2$. Moreover, $2\rho_{n-1}-a_n^2=2\rho_{n-1}-\rho_{n-1}(w^{2j}+w^{-2j}+2)=-\rho_{n-1}(w^{2j}+w^{-2j})=-a_{n-1}$. Then

$$x^4-a_{n-1}x^2+\rho_{n-1}^2=\left(x^2+a_nx+\rho_{n-1}\right)\left(x^2-a_nx+\rho_{n-1}\right),$$

We note ρ_{n-1} ranges over $\Omega(2^{n-1})$ if and only if $-\rho_{n-1}$ ranges over $\Omega(2^{n-1})$ for $n\geq3$. This implies that,

$$Q_{2^n5}(x)=\prod_{\rho_n\in\Omega(2^n)}\prod_{\substack{a_n=\rho_n(w^j+w^{-j})\\ j=1,2}}\left(x^2+a_nx+\rho_n^2\right),$$

for any $3\leq n<L_1$. Similarly, for $n=L_2$, we have $Q_{2^n5}(x)=Q_{2^{L_2-1}5}(x^2)$. Let $\left(x^4+a_{L_2-1}x^2+\rho_{L_2-1}^2\right)=\left(x^2+a_{L_2}x+\rho_{L_2-1}\right)\left(x^2-a_{L_2}x+\rho_{L_2-1}\right)$ where $a_{L_2},\rho_{L_2-1}\in\mathbb{F}_q$. Hence $a_{L_2}^2=2\rho_{L_2-1}-a_{L_2-1}$. Since

$2\rho_{L_2-1}-\rho_{L_2-1}(w^j+w^{-j})=-\rho_{L_2-1}(w^{3j}-w^{-3j})^2\in\mathbb{F}_q$ and both ρ_{L_2-1} and $-(w^{3j}-w^{-3j})^2$ are non-square elements in $\mathbb{F}_q$, there exist $a_{L_2}\in\mathbb{F}_q$ such that $a_{L_2}^2=2\rho_{L_2-1}-a_{L_2-1}$. Note that $L_1=L_2-1$, we have

$$Q_{2^{L_2}5}(x)=\prod_{\rho_{L_1}\in\Omega(2^{L_1})}\prod_{\substack{a_{L_1}=\rho_{L_1}(w^j+w^{-j})\\ j=1,2}}\prod_{a_{L_2}^2=2\rho_{L_1}-a_{L_1}}\left(x^2+a_{L_2}x+\rho_{L_1}\right).$$

For $n=4$, then the result follows from Lemma 1.1 and $Q_{2^n5}(x)=Q_{2^{L_2}5}(x^{2^{n-L_2}})$. For $n>4$, the results follows from Theorem 2.2. Hence

$$Q_{2^n5}(x)=\prod_{\rho_{L_1}\in\Omega(2^{L_1})}\prod_{\substack{a_{L_2}^2=\rho_{L_1}(2-w^j-w^{-j})\\ j=1,2}}\left(x^{2^{n-L_2+1}}+a_{L_2}x^{n-L_2}+\rho_{L_1}\right).$$

□

Theorem 3.5. *Let $q=20k+19$, $w\in\Omega(5)$ be fixed, and $\rho_2=\rho_n^{2^{n-2}}$. Then we have the following factorization of $Q_{2^n5}(x)$ over $\mathbb{F}_q$.*

(i) for $n=0,1$, we have

$$Q_5(x)=\prod_{j=1,2}\left(x^2-(w^j+w^{-j})x+1\right),\ Q_{10}(x)=\prod_{j=1,2}\left(x^2+(w^j+w^{-j})x+1\right).$$

(ii)

$$Q_{20}(x)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2w^j+(\rho_2w^j)^{-1}\\ j=1,2}}\left(x^2+a_2x+1\right).$$

(iii) if $3\le n<L_2$, then

$$Q_{2^n5}(x)=\prod_{\rho_n\in\Omega(2^n)}\prod_{\substack{a_n=\rho_2\rho_nw^j+(\rho_2\rho_nw^j)^{-1}\\ j=1,2}}\left(x^2+a_nx+1\right).$$

(iv) if $n\ge L_2$, then

$$Q_{2^n5}(x)=\prod_{\rho_{L_2}\in\Omega(2^{L_2})}\prod_{\substack{a_{L_2}=\rho_2\rho_{L_2}w^j-(\rho_2\rho_{L_2}w^j)^{-1}\\ j=1,2}}\left(x^{2^{n-L_2+1}}+a_{L_2}x^{2^{n-L_2}}-1\right).$$

In particular, if k is even then $L_2=3$ and for any $n\ge3$,

$$Q_{2^n5}(x)=\prod_{\rho_3\in\Omega(2^3)}\prod_{\substack{a_3=\rho_2\rho_3w^j-(\rho_2\rho_3w^j)^{-1}\\ j=1,2}}\left(x^{2^{n-2}}+a_3x^{2^{n-3}}-1\right).$$

Proof. In this case, $L_1=1$, $L_2=3+v_2(k+1)$, and $L_4=L_2+1$. Again, $5\nmid q-1$ implies that if $w\in\Omega(5)$ then $w\notin\mathbb{F}_q$. However, $w\in\mathbb{F}_{q^2}$. Moreover, -1 is a non-square element. Again, it is trivial to obtain

$$Q_5(x)=\prod_{j=1,2}\left(x^2-(w^j+w^{-j})x+1\right),\ Q_{10}(x)=\prod_{j=1,2}\left(x^2+(w^j+w^{-j})x+1\right).$$

Let a_1 denotes w^j+w^{-j} for $j=1$ or 2. The assumption $q\equiv19\pmod{20}$ forces that we have $(\rho_2w^j)^{q+1}=1$ and thus $\rho_2w^j+(\rho_2w^j)^{-1}=\rho_2w^j+(\rho_2w^j)^q\in\mathbb{F}_q$. Moreover,

$$x^4+a_1x^2+1=(x^2+a_2x+1)(x^2-a_2x+1),$$

where $a_2=\rho_2(w^{3j}-w^{-3j})=\rho_2w^{3j}+(\rho_2w^{3j})^{-1}\in\mathbb{F}_q$. Therefore,

$$Q_{20}(x)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2(w^j-w^{-j})\\ j=1,2}}\left(x^2+a_2x+1\right)=\prod_{\rho_2\in\Omega(2^2)}\prod_{\substack{a_2=\rho_2w^j+(\rho_2w^j)^{-1}\\ j=1,2}}\left(x^2+a_2x+1\right).$$

If k is even then $L_2 = 3$. For $n = 3$, let $\rho_3^2 = \rho_2$ and $a_3 = \rho_2\rho_3 w^{3j} - (\rho_2\rho_3 w^{3j})^{-1}$. We claim that that $a_3 \in \mathbb{F}_q$. First, we note that $\rho_2^q = \rho_2^{-1}$, and $w^{qj} = w^{-j}$. Moreover, $\rho_3^q = -\rho_3^{-1}$ because $\rho_3^{2(q+1)} = 1$ and $\rho_3^{q+1} \neq 1$. Then

$$a_3^q = (\rho_2\rho_3 w^{3j} - (\rho_2\rho_3 w^{3j})^{-1})^q = \rho_2^q\rho_3^q w^{3jq} - \rho_2^{-q}\rho_3^{-q} w^{-3jq} = (\rho_2^{-1})(-\rho_3^{-1})w^{-3j} - (\rho_2(-\rho_3)w^{3j}) = a_3$$

Moreover, $(x^2+a_3x-1)(x^2-a_3x-1) = x^4+a_2x+1$ holds as a consequence of $a_3^2 = -\rho_2 w^j - \rho_2^{-1}w^{-j} - 2 = -a_2 - 2$. Hence

$$Q_{40}(x) = \prod_{\rho_3\in\Omega(2^3)} \prod_{\substack{a_3=\rho_2\rho_3 w^j - (\rho_2\rho_3 w^j)^{-1} \\ j=1,2}} \left(x^2 + a_3x - 1\right).$$

The rest of proof for even k follows from Lemma 1.1 and $Q_{2^n5}(x) = Q_{40}(x^{2^{n-3}})$.

If k is odd, then $L_2 > 3$. For any $3 \le n < L_2$, we have $\rho_n^{q+1} = 1$. This implies that $(\rho_2\rho_n w^j)^{q+1} = 1$. Hence $a_n = \rho_2\rho_n w^j + (\rho_2\rho_n w^j)^{-1} = \rho_2\rho_n w^j + (\rho_2\rho_n w^j)^q \in \mathbb{F}_q$. Since $2 - a_3^2 = 2 - (\rho_2\rho_3 w^{3j} + (\rho_2\rho_3 w^{3j})^{-1})^2 = \rho_2 w^j + (\rho_2 w^j)^{-1} = a_2$, we have $x^4 + a_2x^2 + 1 = (x^2 + a_3x + 1)(x^2 - a_3x + 1)$, and thus

$$Q_{40}(x) = \prod_{\rho_3\in\Omega(2^3)} \prod_{\substack{a_3=\rho_2\rho_3 w^j + (\rho_2\rho_3 w^j)^{-1} \\ j=1,2}} \left(x^2 + a_3x + 1\right).$$

We note that ρ_{n-1} ranges over $\Omega(2^{n-1})$ if and only if $\rho_2\rho_{n-1}$ ranges over $\Omega(2^{n-1})$ for $n \ge 4$. Indeed, for $n \ge 4$, we have $(\rho_2\rho_{n-1})^{2^{n-1}} = (\rho_{n-1})^{2^{n-1}} = 1$ and $(\rho_2\rho_{n-1})^{2^{n-2}} = (\rho_{n-1})^{2^{n-2}} \neq 1$. This simplifies that

$$Q_{40}(x) = \prod_{\rho_3\in\Omega(2^3)} \prod_{\substack{a_3=\rho_3 w^j + (\rho_3 w^j)^{-1} \\ j=1,2}} \left(x^2 + a_3x + 1\right).$$

Now we can see that $2 - a_n^2 = 2 - (\rho_2\rho_n w^{3j} + (\rho_2\rho_n w^{3j})^{-1})^2 = \rho_{n-1}w^j + (\rho_{n-1}w^j)^{-1}$ is one of a_{n-1}'s as ρ_{n-1} ranges over $\Omega(2^{n-1})$ for $n \ge 4$. Therefore

$$\begin{aligned} Q_{2^n5}(x) = Q_{2^{n-1}5}(x^2) &= \prod_{\rho_{n-1}\in\Omega(2^{n-1})} \prod_{\substack{a_{n-1}=\rho_2\rho_{n-1}w^j + (\rho_2\rho_{n-1}w^j)^{-1} \\ j=1,2}} \left(x^4 + a_{n-1}x^2 + 1\right) \\ &= \prod_{\rho_n\in\Omega(2^n)} \prod_{\substack{a_n=\rho_2\rho_n w^j + (\rho_2\rho_n w^j)^{-1} \\ j=1,2}} \left(x^2 + a_nx + 1\right) \\ &= \prod_{\rho_n\in\Omega(2^n)} \prod_{\substack{a_n=\rho_n w^j + (\rho_n w^j)^{-1} \\ j=1,2}} \left(x^2 + a_nx + 1\right) \end{aligned}$$

if k is odd and $4 \le n < L_2$. This completes the proof of (iii).

Finally, for $n = L_3$, let $\rho_{L_2}^2 = \rho_{L_2-1}$ and $a_{L_2} = \rho_2\rho_{L_2}w^{3j} - (\rho_2\rho_{L_2}w^{3j})^{-1}$. We claim that that $a_{L_2} \in \mathbb{F}_q$. First, we note that $\rho_2^q = \rho_2^{-1}$, and $(w^j)^q = w^{-j}$. Moreover, $\rho_{L_2}^q = -\rho_{L_2}^{-1}$ holds because $\rho_{L_2}^{2(q+1)} = 1$ and $\rho_{L_2}^{q+1} \neq 1$. Then

$$a_{L_2}^q = (\rho_2\rho_{L_2}w^{3j} - (\rho_2\rho_{L_2}w^{3j})^{-1})^q = \rho_2^q\rho_{L_2}^q w^{3jq} - \rho_2^{-q}\rho_{L_2}^{-q}w^{-3jq} = (\rho_2^{-1})(-\rho_{L_2}^{-1})w^{-3j} - (\rho_2(-\rho_{L_2})w^{3j}) = a_{L_2}$$

Since $a_{L_2}^2 = -\rho_{L_2-1}w - \rho_{L_2-1}^{-1}w^{-1} - 2 = -a_{L_2-1} - 2$ for a different choice of ρ_{L_2-1}, we can verify easily that $(x^2 + a_{L_2}x - 1)(x^2 - a_{L_2}x - 1) = x^4 + a_{L_2-1}x + 1$. Hence

$$Q_{2^{L_2}5}(x) = \prod_{\rho_{L_2}\in\Omega(2^{L_2})} \prod_{\substack{a_{L_2}=\rho_2\rho_{L_2}w^j - (\rho_2\rho_{L_2}w^j)^{-1} \\ j=1,2}} \left(x^2 + a_{L_2}x - 1\right).$$

The rest of proof of (v) follows from Lemma 1.1 and $Q_{2^n5}(x) = Q_{2^{L_2}}(x^{2^{n-L_2}})$.

□

Again, we can reformulate the previous two results as follows:

Corollary 3.6. *Let $q \equiv 9, 19 \pmod{20}$. Let $w \in \Omega(5)$ be fixed. For any $2 \le n \le L_2$, we have*

$$Q_{2^n5}(x) = \prod_{a_n, b_n} \left(x^2 + a_n x + b_n\right),$$

where a_n, b_n are all the solutions to the system of nonlinear recurrence relations

$$\begin{cases} a_n^2 &= 2b_n - a_{n-1} \\ b_n^2 &= b_{n-1}, \end{cases}$$

for initial values $(a_1, b_1) = (w + w^{-1}, 1)$ and $(a_1, b_1) = (w^2 + w^{-2}, 1)$. For $n > L_2$,

$$Q_{2^n5}(x) = \prod_{a_{L_2}, b_{L_2}} \left(x^{2^{n-L_2+1}} + a_{L_2} x^{2^{n-L_2}} + b_{L_2}\right).$$

Finally we give the following classes of irreducible binomials and trinomials.

Corollary 3.7. *Let $w \in \Omega(5)$, $L_1 = v_2(q-1)$, $L_2 = L_1 + v_2(q+1)$, and $\rho_n \in \Omega(2^n)$ where $\rho_2 = \rho_n^{2^{n-2}}$.*

(i) $f(x) = x^{n-L_1} - w\rho_{L_1}$ is irreducible over $\mathbb{F}_q$ for any $q \equiv 1 \pmod{20}$ and any $n \ge L_2$;

(ii) $f(x) = x^{2^{n-L_2+1}} - (\rho_{L_2} - \rho_{L_2}^{-1}) w x^{2^{n-L_2}} - w^2$ is irreducible over $\mathbb{F}_q$ for any $q \equiv 11 \pmod{20}$ and any $n \ge L_2$;

(iii) $f(x) = x^{2^{n-L_2+1}} + a_{L_2} x^{2^{n-L_2}} + \rho_{L_1}$ is irreducible over $\mathbb{F}_q$ for any $q \equiv 9 \pmod{20}$, any $n \ge L_2$, and any a_{L_2} satisfying $a_{L_2}^2 = 2\rho_{L_1} - \rho_{L_1}(w + w^{-1})$;

(iv) $f(x) = x^{2^{n-L_2+1}} + a_{L_2} x^{2^{n-L_2}} - 1$ is irreducible over $\mathbb{F}_q$ for any $q \equiv 19 \pmod{20}$, any $n \ge L_2$, and any a_{L_2} satisfying $a_{L_2}^2 = \rho_2 \rho_{L_2} w - (\rho_2 \rho_{L_2} w)^{-1}$,

4. The case $q \equiv \pm 2 \pmod 5$ and $q \equiv 1 \pmod 4$

We note that if $q \equiv \pm 2 \pmod 5$ and $q \equiv 1 \pmod 4$ (i.e., $q \equiv 13 \pmod{20}$ or $q \equiv 17 \pmod{20}$), then $L_4 = L_2 + 1$ and $L_2 = L_1 + 1$. Moreover, $\rho_1 = -1$ must be a square and thus there exists $\rho_2 \in \mathbb{F}_q$ such that $\rho_2^2 = \rho_1$.

Theorem 4.1. *Let $q \equiv \pm 2 \pmod 5$ and $q \equiv 1 \pmod 4$. Then we have the following factorization of 2^n5-th cyclotomic polynomial $Q_{2^n5}(x)$ over $\mathbb{F}_q$.*

(i) If $0 \le n \le L_1$, then

$$Q_{2^n5}(x) = \prod_{\rho_n \in \Omega(2^n)} \left(x^4 + \rho_n x^3 + \rho_n^2 x^2 + \rho_n^3 x + \rho_n^4\right).$$

(ii) If $n = L_2$ (i.e., $L_2 = L_1 + 1$), then

$$Q_{2^n5}(x) = \prod_{\rho_{n-1} \in \Omega(2^{n-1})} \prod_{a_n^2 = 5\rho_{n-1}} \left(x^4 + a_n x^3 + 3\rho_{n-1} x^2 + a_n \rho_{n-1} x + \rho_{n-1}^2\right).$$

(iii) If $n \ge L_4 = L_2 + 1$, then $Q_{2^n5}(x)$ can be factorized as

$$\begin{cases} \displaystyle\prod_{\rho_{L_1} \in \Omega(2^{L_1})} \prod_{a_{L_2}^2 = 5\rho_{L_1}} \prod_{a_{L_4}^2 = (2\rho_2 - 1)a_{L_2}} \left(x^{2^{n-L_4+2}} + a_{L_4} x^{3 \cdot 2^{n-L_4}} + a_{L_2}\rho_2 x^{2^{n-L_4+1}} + (-5\rho_{L_1}) a_{L_4}^{-1} x^{2^{n-L_4}} - \rho_{L_1}\right), \\ \qquad\qquad if\ (2\rho_2 - 1)a_{L_2}\ is\ a\ square; \\ \displaystyle\prod_{\rho_{L_1} \in \Omega(2^{L_1})} \prod_{a_{L_2}^2 = 5\rho_{L_1}} \prod_{a_{L_4}^2 = -(2\rho_2 + 1)a_{L_2}} \left(x^{2^{n-L_4+2}} + a_{L_4} x^{3 \cdot 2^{n-L_4}} + (-a_{L_2}\rho_2) x^{2^{n-L_4+1}} + (-5\rho_{L_1}) a_{L_4}^{-1} x^{2^{n-L_4}} - \rho_{L_1}\right), \\ \qquad\qquad if\ (2\rho_2 - 1)a_{L_2}\ is\ a\ non-square. \end{cases}$$

Proof. Since the smallest positive d satisfying $q^d \equiv 1 \pmod 5$ is 4 under our assumption, by Theorem 2.47 in [8], for all $0 \le n \le L_4$, $Q_{2^n 5}$ factors into a product of $\phi(2^n 5)/4 = 2^{n-1}$ distinct monic irreducible polynomials of degree 4.

(i) If $n \le L_1$, then $\rho_n \in \Omega(2^n) \subseteq \mathbb{F}_q$. Hence $x^4 + \rho_n x^3 + \rho_n^2 x^2 + \rho_n^3 x + \rho_n^4 \in \mathbb{F}_q[x]$. The factorization of $Q_{2^n 5}(x)$ when $n = 0, 1$ is trivial. Moreover, it is straightforward to verify that for $\rho_n^2 = \rho_{n-1}$

$$x^8 + \rho_{n-1}x^6 + \rho_{n-1}^2 x^4 + \rho_{n-1}^3 x^2 + \rho_{n-1}^4 = \left(x^4 + \rho_n x^3 + \rho_n^2 x^2 + \rho_n^3 x + \rho_n^4\right)\left(x^4 - \rho_n x^3 + \rho_n^2 x^2 - \rho_n^3 x + \rho_n^4\right).$$

Hence (i) follows from $Q_{2^n 5}(x) = Q_{2^{n-1}5}(x^2)$ and the consequences of Theorem 2.47 in [8] as mentioned above.

(ii) From (i) and Lemma 2.1, we have

$$Q_{2^{L_2}5}(x) = Q_{2^{L_1}5}(x^2) = \prod_{\rho_{L_1} \in \Omega(2^{L_1})} \left(x^8 + \rho_{L_1} x^6 + \rho_{L_1}^2 x^4 + \rho_{L_1}^3 x^2 + \rho_{L_1}^4\right).$$

Here 5 is a non-square in $\mathbb{F}_q$ under the assumption of our theorem due to the fact that the Legendre symbol $\left(\frac{5}{p}\right) = 1$ iff $p \equiv \pm 1, \pm 9 \pmod{20}$. Hence $5\rho_{L_1}$ is a square element in $\mathbb{F}_q$ as ρ_{L_1} is also a non-square element in $\mathbb{F}_q$. Let $a_{L_2}^2 = 5\rho_{L_1}$. Then $\pm a_{L_2} \in \mathbb{F}_q$. Hence $x^4 \pm a_{L_2} x^3 + 3\rho_{L_1} x^2 \pm a_{L_2}\rho_{L_1} x + \rho_{L_1 - 1} \in \mathbb{F}_q[x]$. One can also easily verify that

$$x^8 + \rho_{L_1} x^6 + \rho_{L_1}^2 x^4 + \rho_{L_1}^3 x^2 + \rho_{L_1}^4 = \prod_{a_{L_2}^2 = 5\rho_{L_1}} \left(x^4 + a_{L_2} x^3 + 3\rho_{L_1} x^2 + a_{L_2}\rho_{L_1} x + \rho_{L_1}^2\right).$$

Therefore the rest of proof of (ii) follows.

(iii) We first consider $n = L_4$. Since $L_4 = L_2 + 1$, we essentially need to factor $x^8 + a_{L_2} x^6 + 3\rho_{L_1} x^4 + a_{L_2}\rho_{L_1} x^2 + \rho_{L_1 - 1}$ into two monic quartic polynomials in $\mathbb{F}_q[x]$, where $\rho_{L_1} \in \Omega(2^{L_1})$ and $a_{L_2}^2 = 5\rho_{L_1}$.

Again -1 is a square element and 5 is a non-square imply that $-(2\rho_2 + 1)a_{L_2}(2\rho_2 - 1)a_{L_2} = -(4\rho_2^2 - 1)a_{L_2}^2 = 5a_{L_2}^2$ is a non-square element in $\mathbb{F}_q$. Hence either $-(2\rho_2 + 1)a_{L_2}$ or $(2\rho_2 - 1)a_{L_2}$ (exactly one of them) is a square element in $\mathbb{F}_q$.

If $(2\rho_2 - 1)a_{L_2}$ is a square, we let $a_{L_4}^2 = (2\rho_2 - 1)a_{L_2}$. Then

$$x^8 + a_{L_2} x^6 + 3\rho_{L_1} x^4 + a_{L_2}\rho_{L_1} x^2 + \rho_{L_1}^2 = \prod_{a_{L_4}^2 = (2\rho_2 - 1)a_{L_2}} \left(x^4 + a_{L_4} x^3 + \rho_2 a_{L_2} x^2 + (-5\rho_{L_1})a_{L_4}^{-1} x - \rho_{L_1}\right)$$

If $(2\rho_2 - 1)a_{n-1}$ is a non-square then $-(2\rho_2 + 1)a_{L_2}$ is a square. In this case, we let $a_{L_4}^2 = -(2\rho_2 + 1)a_{L_2}$. Then

$$x^8 + a_{L_2} x^6 + 3\rho_{L_1} x^4 + a_{L_2}\rho_{L_1} x^2 + \rho_{L_1}^2 = \prod_{a_{L_4}^2 = -(2\rho_2 + 1)a_{L_2}} \left(x^4 + a_{L_4} x^3 - \rho_2 a_{L_2} x^2 + (-5\rho_{L_1})a_{L_4}^{-1} x - \rho_{L_1}\right)$$

Since each quartic polynomial is in $\mathbb{F}_q[x]$ and $Q_{2^{L_4}5}(x)$ factors into product of quartic polynomials, every such quartic polynomial must be irreducible. Hence (iii) is proved for $n = L_4$. The rest of proof follows from Theorem 2.2. □

Corollary 4.2. *Let $q \equiv \pm 2 \pmod 5$ and $q \equiv 1 \pmod 4$. Let $\rho_n \in \Omega(2^n)$, $\rho_n^{2^{n-2}} = \rho_2$, and $a_{L_2}^2 = 5\rho_{L_1}$.*

(i) If $2(\rho_2 - 1)a_{L_2}$ is a square, then $x^{2^{n-L_4+2}} + a_{L_4} x^{3\cdot 2^{n-L_4}} + a_{L_2}\rho_2 x^{2^{n-L_4+1}} + (-5\rho_{L_1})a_{L_4}^{-1} x^{2^{n-L_4}} - \rho_{L_1}$ is irreducible over $\mathbb{F}_q$ for each choice of ρ_n, a_{L_2}, and $a_{L_4}^2 = (2\rho_2 - 1)a_{L_2}$;

(ii) otherwise, $x^{2^{n-L_4+2}} + a_{L_4} x^{3\cdot 2^{n-L_4}} + (-a_{L_2}\rho_2) x^{2^{n-L_4+1}} + (-5\rho_{L_1})a_{L_4}^{-1} x^{2^{n-L_4}} - \rho_{L_1}$ is irreducible over $\mathbb{F}_q$ for each choice of ρ_n, a_{L_2}, and $a_{L_4}^2 = -(2\rho_2 + 1)a_{L_2}$.

5. The case $q \equiv \pm 2 \pmod 5$ and $q \equiv 3 \pmod 4$

We note that if $q \equiv \pm 2 \pmod 5$ and $q \equiv 3 \pmod 4$ (i.e., $q \equiv 3 \pmod{20}$ or $q \equiv 7 \pmod{20}$), then $L := L_4 = L_2 + 1$ and $L_1 = 1$. However, $L_2 = 3 + v_2(5k+1)$ for $q = 20k+3$ and $L_2 = 3 + v_2(5k+3)$ for $q = 20k+7$.

Theorem 5.1. *Let $q \equiv \pm 2 \pmod 5$ and $q \equiv 3 \pmod 4$. Then we have the following factorization of $Q_{2^n 5}(x)$ over $\mathbb{F}_q$.*

(i) If $0 \le n \le 1$, then

$$Q_{2^n 5}(x) = \prod_{\rho_n \in \Omega(2^n)} \left(x^4 + \rho_n x^3 + \rho_n^2 x^2 + \rho_n^3 x + \rho_n^4\right).$$

(ii) If $2 \le n \le L_2$, then

$$Q_{2^n 5}(x) = \prod_{a_n, b_n, c_n} \left(x^4 + a_n x^3 + b_n x^2 + c_n x + 1\right),$$

where a_n, b_n, c_n satisfies the following system of nonlinear recurrence relations

$$\begin{cases} 2b_n - a_n^2 &= a_{n-1} \\ 2 + b_n^2 - 2a_n c_n &= b_{n-1} \\ 2b_n - c_n^2 &= c_{n-1}, \end{cases}$$

for initial values $a_1 = -1$, $b_1 = 1$, and $c_1 = -1$.

(iii) If $n \ge L = L_4 = L_2 + 1$, then

$$Q_{2^n 5}(x) = \prod_{a_L, b_L, c_L} \left(x^{2^{n-L+2}} + a_L x^{3\cdot 2^{n-L}} + b_L x^{2^{n-L+1}} + c_L x^{2^{n-L}} - 1\right),$$

where a_L, b_L, c_L satisfies the following system of nonlinear recurrence relations

$$\begin{cases} 2b_L - a_L^2 &= a_{L-1} \\ -2 + b_L^2 - 2a_L c_L &= b_{L-1} \\ -2b_L - c_L^2 &= c_{L-1}, \end{cases}$$

for each triple $a_{L-1}, b_{L-1}, c_{L-1}$ obtained in (ii).

Proof. (i) Under the assumptions that $q \equiv \pm 2 \pmod 5$ and $q \equiv 3 \pmod 4$, $Q_{2^n 5}(x)$ factors into a product of $\phi(2^n 5)/4 = 2^{n-1}$ distinct monic irreducible polynomials of degree 4. It is trivial to check $Q_5(x) = \prod_{w \in \Omega(5)}(x - w) = x^4 + x^3 + x^2 + x + 1$ and $Q_{10}(x) = Q_5(-x) = x^4 - x^3 + x^2 - x + 1$.

(ii) Since $Q_{2^n 5}(x) = Q_{2^{n-1}5}(x^2)$, it is enough to study the factors of $x^8 + a_{n-1}x^6 + b_{n-1}x^4 + c_{n-1}x^2 + 1$. Again, the consequence that each irreducible factor of $Q_{2^n 5}(x)$ has degree 4 simplifies the problem and thus we only need to consider the following irreducible factorization

$$\begin{aligned} & x^8 + a_{n-1}x^6 + b_{n-1}x^4 + c_{n-1}x^2 + 1 \\ = \;& \left(x^4 + d_3 x^3 + d_2 x^2 + d_1 x + d_0\right)\left(x^4 + e_3 x^3 + e_2 x^2 + e_1 x + e_0\right) \end{aligned}$$

Since all the roots of an irreducible factor are the conjugates of a primitive $2^n r$-th root of unity, d_0 and e_0 are of form $\beta^{1+q+q^2+q^3}$ for some primitive $2^n r$-th root of unity β. Under our assumptions, $5 \mid 1 + q + q^2 + q^3$. Moreover, $v_2(1 + q + q^2 + q^3) = v_2(q+1) + 1 = L_2$. This implies that for $2 \le n \le L_2$ we have $2^n 5 \mid 1 + q + q^2 + q^3$. Hence $d_0 = e_0 = 1$. Then one can easily show that $e_3 = -d_3$ and $e_1 = -d_1$ because coefficients of x^7 and x vanish in the product. This forces that $d_2 = e_2$. Hence we have

$$\begin{aligned} & x^8 + a_{n-1}x^6 + b_{n-1}x^4 + c_{n-1}x^2 + 1 \\ = \;& \left(x^4 + a_n x^3 + b_n x^2 + c_n x + 1\right)\left(x^4 - a_n x^3 + b_n x^2 - c_n x + 1\right) \end{aligned}$$

By comparing both sides of the above equation, we conclude a_n, b_n, c_n $(2 \le n \le L_2)$ must satisfy the following system of nonlinear recurrence relations

$$\begin{cases} 2b_n - a_n^2 &= a_{n-1} \\ 2 + b_n^2 - 2a_n c_n &= b_{n-1} \\ 2b_n - c_n^2 &= c_{n-1}. \end{cases}$$

We note that the above system has exactly two solutions for each n due to the fact that the factorization is unique,

(iii) For $n = L = L_2 + 1$, we have $2^L r \nmid 1 + q + q^2 + q^3$. But $2^{L_2} r \mid 1 + q + q^2 + q^3$ implies that $d_0 = e_0 = -1$. So we must have

$$\begin{aligned} & x^8 + a_{n-1}x^6 + b_{n-1}x^4 + c_{n-1}x^2 + 1 \\ = \; & \left(x^4 + a_n x^3 + b_n x^2 + c_n x - 1\right)\left(x^4 - a_n x^3 + b_n x^2 - c_n x - 1\right) \end{aligned}$$

Hence a_L, b_L, c_L satisfy the following system of nonlinear recurrence relations

$$\begin{cases} 2b_L - a_L^2 &= a_{L-1} \\ -2 + b_L^2 - 2a_L c_L &= b_{L-1} \\ -2b_L - c_L^2 &= c_{L-1}, \end{cases}$$

for each triple $a_{L-1}, b_{L-1}, c_{L-1}$ obtained in (ii). The rest of proof follows from Theorem 2.2. □

We note that if $q \equiv 3 \pmod{20}$ and k is even, or, $q \equiv 7 \pmod{20}$ and k is odd, then $L = 4$. So the factorization over these fields is very fast. We also note that for small n's the solutions (a_n, b_n, c_n) of the above systems of nonlinear recurrence relations can be explicitly expressed in some cases. For example, for $q \equiv 3 \pmod{20}$ and $q > 3$, the solutions (a_2, b_2, c_2) satisfy that $a_2^2 = -5$, $b_2 = 3\rho_1$, $c_2 = a_2\rho_1$. If k is even, then $a_3^2 = 2 - a_2$, $b_3 = 1$, and $c_3 = 3a_3^{-1}$; if k is odd, then $a_3^2 = -2 - a_2$, $b_3 = -1$, and $c_3 = 3a_3^{-1}$. For $q \equiv 7 \pmod{20}$, if k is odd, then $a_3^2 = 2 - a_2$, $b_3 = 1$, and $c_3 = 3a_3^{-1}$; if k is even, then $a_3^2 = -2 - a_2$, $b_3 = -1$, and $c_3 = 3a_3^{-1}$.

Corollary 5.2. *Let $q \equiv \pm 2 \pmod{5}$ and $q \equiv 3 \pmod{4}$. Denote $L = v_2(q^4 - 1)$. Let $a_1 = -1$, $b_1 = 1$, and $c_1 = -1$. For each a_L, b_L, c_L satisfying*

$$\begin{cases} 2b_L - a_L^2 &= a_{L-1} \\ -2 + b_L^2 - 2a_L c_L &= b_{L-1} \\ -2b_L - c_L^2 &= c_{L-1}, \end{cases}$$

and

$$\begin{cases} 2b_m - a_m^2 &= a_{m-1} \\ 2 + b_m^2 - 2a_m c_m &= b_{m-1} \\ 2b_m - c_m^2 &= c_{m-1}, \end{cases}$$

where $2 \le m \le L - 1$, the polynomial

$$x^{2^{n-L+2}} + a_L x^{3 \cdot 2^{n-L}} + b_L x^{2^{n-L+1}} + c_L x^{2^{n-L}} - 1$$

is irreducible over $\mathbb{F}_q$ for any $n \ge L$.

Finally we use some examples to illustrate our results. We provide the following tables for coefficients (a_n, b_n, c_n) appeared in the factorization of $Q_{2^n 5}(x)$ over $\mathbb{F}_q$ where $q = 7$ or 67. We note that (a_n, b_n, c_n)'s are computed using MAPLE programs, which are simple implementations of solving the systems of nonlinear recurrence relations as stated in Theorem 5.1.

TABLE 1. Factorization of $Q_{2^n5}(x)$ over $\mathbb{F}_q$ where $q = 7$ (k is even, $L_4 = 5$)

n	1	2	3	4	5
(a_n, b_n, c_n)	$(-1, 1, 1)$	$(3, 4, 4)$ $(4, 4, 3)$	$(3, 6, 1)$ $(4, 6, 6)$ $(1, 6, 3)$ $(6, 6, 4)$	$(0, 5, 3)$ $(0, 5, 4)$ $(2, 4, 3)$ $(5, 4, 4)$ $(3, 5, 0)$ $(4, 5, 0)$ $(3, 4, 2)$ $(4, 4, 5)$	$(0, 0, 2)$ $(0, 0, 5)$ $(3, 1, 6)$ $(4, 1, 1)$ $(1, 5, 6)$ $(6, 5, 1)$ $(1, 3, 5)$ $(6, 3, 2)$ $(2, 0, 0)$ $(5, 0, 0)$ $(6, 6, 3)$ $(1, 6, 4)$ $(1, 2, 6)$ $(6, 2, 1)$ $(5, 4, 1)$ $(2, 4, 6)$

TABLE 2. Factorization of $Q_{2^n5}(x)$ over $\mathbb{F}_q$ where $q = 67$ (k is odd, $L_4 = 4$)

n	1	2	3	4
(a_n, b_n, c_n)	$(-1, 1, 1)$	$(14, 64, 53)$ $(53, 64, 14)$	$(16, 1, 63)$ $(51, 1, 4)$ $(4, 1, 51)$ $(63, 1, 16)$	$(21, 61, 63)$ $(46, 61, 4)$ $(33, 34, 53)$ $(34, 34, 14)$ $(14, 33, 34)$ $(53, 33, 33)$ $(4, 6, 16)$ $(63, 6, 21)$

6. CONCLUSION

In this paper, we obtain the explicit factorization of cyclotomic polynomials of $Q_{2^n r}(x)$ over finite fields where $r = 5$ and construct several classes of irreducible polynomials of degree 2^{n-2} with fewer than 5 terms. Our approach is recursive, i.e., we derive the factorization of $Q_{2^k r}(x)$ from the factorization of $Q_{2^{k-1}r}(x^2)$. We show that we can do it with at most $L_{\phi(r)} = v_2(q^{\phi(r)} - 1)$ iterations. A key component of our approach for $r = 5$ is to factor certain types of polynomials of degree 8 into two quartic irreducible polynomials. It would be more desirable to obtain explicit factors of $Q_{2^n r}(x)$ for arbitrary r. One would expect that it involves the factorization of certain types of polynomials of degree $2m$ where $m \mid \phi(r)$ into a product irreducible polynomials of degree less than or equal to m. Another contribution of this paper is the construction of several classes of irreducible polynomials over finite fields with at most 5 nonzero terms. We note that one can also construct more classes of irreducible polynomials for other choices of r as a consequence of Theorem 2.2.

Acknowledgments

Part of the work was done while Qiang Wang took his sabbatical leave at the Center for Advanced Study, Tsinghua University. He wants to thank the Center for its warm hospitality. We also want to thank the anonymous referees for many valuable suggestions to improve the results of this paper.

References

[1] E. R. Berlekamp, Bit-serial Reed-Solomon encoders, *IEEE Trans. Info. Theory* **28** (1982), 869-874.
[2] F. R. Beyl, Cyclic subgroups of the prime residue group, *Amer. Math. Monthly* **84** (1977), 46-48.
[3] S. D. Cohen, Explicit theorems on generator polynomials, *Finite Fields Appl.* **11** (2005), 337-357.
[4] R. W. Fitzgerald and J. L. Yucas, Factors of Dickson polynomials over finite fields, *Finite Fields Appl.* **11** (2005), 724-737.
[5] R. W. Fitzgerald and J. L. Yucas, Explicit Factorization of Cyclotomic and Dickson polynomials over Finite Fields, Arithmetic of finite fields, *Lecture Notes in Comput. Sci.* **4547**, Springer, Berlin, 2007, 1-10.
[6] S. Gao, J. Howell, D. Panario, Irreducible polynomials of given forms, *Contemp. Math.* **225** (1999), 43-54.
[7] S. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005.
[8] R. Lidl and H. Niederreiter, Finite Fields, in Encyclopedia of Mathematics and Its Application, 2nd edn., vol 20, Cambridge University Press, Cambridge, 1997.
[9] H. Meyn, Factorization of the cyclotomic polynomials $x^{2^n}+1$ over finite fields, *Finite Fields Appl.* **2** (1996), 439-442.
[10] M. Wang and I. F. Blake, Bit-serial multiplication in finite fields, *IEEE Trans. Comput.* **38** (1989), 1457-1460.

Center for Advanced Study, Tsinghua University, HaiDian District, Beijing(100084), China.
E-mail address: wanglp@mail.tsinghua.edu.cn

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.
E-mail address: wang@math.carleton.ca