Journal of Number Theory 188 (2018) 229–246

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the roots of certain Dickson polynomials ☆

Aart Blokhuis [a], Xiwang Cao [b,c], Wun-Seng Chou [d,*], Xiang-Dong Hou [e]

[a] *Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*
[b] *School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*
[c] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[d] *Institute of Mathematics, Academia Sinica, and Department of Mathematical Sciences, National Chengchi University, Taipei, Taiwan*
[e] *Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, USA*

A R T I C L E I N F O

Article history:
Received 11 April 2017
Received in revised form 8 January 2018
Accepted 8 January 2018
Available online 2 March 2018
Communicated by D. Wan

Keywords:
Absolutely irreducible
Button madness
Dickson polynomials
Fermat number
Finite field
Reciprocal polynomial

A B S T R A C T

Let n be a positive integer, $q = 2^n$, and let $\mathbb{F}_q$ be the finite field with q elements. For each positive integer m, let $D_m(X)$ be the Dickson polynomial of the first kind of degree m with parameter 1. Assume that $m > 1$ is a divisor of $q+1$. We study the existence of $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$. We also explore the connections of this question to an open question by Wiedemann and a game called "Button Madness".

☆ This work is partially supported both by the NNSF of China under the grants numbers 11771007, 61572027, and by the MOST of Taiwan under the grants number 106-2115-M-001-003.
* Corresponding author.
E-mail addresses: a.blokhuis@tue.nl (A. Blokhuis), xwcao@nuaa.edu.cn (X. Cao), macws@math.sinica.edu.tw (W.-S. Chou), xhou@usf.edu (X.-D. Hou).

https://doi.org/10.1016/j.jnt.2018.01.003

1. Introduction

For each integer $m > 0$, we consider a polynomial $D_m(X)$ defined by

$$D_m(X) = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-1)^i X^{m-2i}.$$

Trivially, $D_m(X) \in \mathbb{Z}[X]$. It is well known that

$$D_m(X + X^{-1}) = X^m + X^{-m}. \tag{1}$$

(For these facts see, for example, [6].) From (1), $D_m \circ D_\ell = D_{m\ell}$ for all integers $m, \ell \geq 0$.

Now, let n be a positive integer, $q = 2^n$, and let $\mathbb{F}_q$ be the finite field with q elements. In this paper, the polynomial $D_m(X)$ is treated as an element of $\mathbb{F}_q[X]$; it is called the *Dickson polynomial of the first kind of degree m with parameter* 1 over $\mathbb{F}_q$ (or simply the *Dickson polynomial of degree m*). Dickson polynomials have been studied extensively and the reader is referred to [7] for more details.

Roots of Dickson polynomials have been studied by several authors; see [2,3] for instance. The work of the present paper was motivated by the following question raised by M. Freedman [4]:

Question 1.1. Is it true that for every divisor $m > 1$ of the jth Fermat number $F_j = 2^{2^j} + 1$, there exists $\alpha \in \mathbb{F}^*_{2^{2^j}}$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$?

We will see that the answer is negative. The first counterexample has $m = 641$ and $j = 5$ as we will see in Section 4. In this paper, we consider the above question in a more general setting: For positive integers m and n with $m \mid (2^n + 1)$, we study the existence of $\alpha \in \mathbb{F}^*_{2^n}$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$. We begin with some preliminary observations. Let $q = 2^n$, $\alpha \in \mathbb{F}_q$, and write $\alpha = \zeta + \zeta^{-1}$, where $\zeta \in \mathbb{F}^*_{q^2}$. It follows from (1) that $D_m(\alpha) = 0$ if and only if $\zeta^m = 1$, i.e., if and only if $X^m + 1 \equiv 0 \pmod{X^2 + \alpha X + 1}$. Therefore, our aim is to determine if there exists $\alpha \in \mathbb{F}^*_q$ such that both $X^2 + \alpha X + 1$ and $X^2 + \alpha^{-1} X + 1$ divide $X^m + 1$. Note that $(X^m + 1) \mid (X^{q+1} + 1)$ and that for $\alpha \in \mathbb{F}^*_q$, $(X^2 + \alpha X + 1) \mid (X^{q+1} + 1)$ if and only if $X^2 + \alpha X + 1$ is irreducible over $\mathbb{F}_q$.

For $u \in \mathbb{F}_{q^t}$, let $T_{q^t|q}(u) = u + u^q + \cdots + u^{q^{t-1}}$ be the trace of u and let $T_{q^t}(u) = T_{q^t|2}(u)$ be the absolute trace of u. The following fact is well-known.

Lemma 1.2. *For $\alpha \in \mathbb{F}^*_q$, $X^2 + \alpha X + 1$ is irreducible over $\mathbb{F}_q$ if and only if $T_q(\alpha^{-1}) = 1$.*

The *reciprocal* $f^*(X)$ of a nonzero polynomial $f(X)$ is defined by $f^*(X) = X^{\deg(f)} f(1/X)$. A polynomial is called *self-reciprocal* if it coincides with its reciprocal. Both $X^2 + \alpha X + 1$ and $X^m + 1$ are self-reciprocal polynomials. Since $m \mid (q + 1)$, we have $(X^m + 1) \mid (X^{q+1} + 1)$. Therefore, it is helpful to know the factors of $X^{q+1} + 1$. Indeed, Meyn [9] has proved the following result.

Lemma 1.3 *([9, Theorem 1]). Let r be a prime power (not necessarily even) and t be a positive integer.*

(i) *Every self-reciprocal irreducible monic polynomial of degree $2t$ over $\mathbb{F}_r$ is a factor of the polynomial $X^{r^t+1}-1$.*
(ii) *Every irreducible factor of degree ≥ 2 of $X^{r^t+1}-1$ over $\mathbb{F}_r$ is a self-reciprocal irreducible monic polynomial of degree $2d$, where d divides t such that t/d is odd.*

By Lemma 1.3, every irreducible factor of degree ≥ 2 of X^m+1 over a subfield K of $\mathbb{F}_q$ is a self-reciprocal monic polynomial of even degree. Note that if $f(X) \in K[X]$ is a polynomial of positive degree k, then $\Phi(f(X)) = X^k f(X+X^{-1})$ is a self-reciprocal polynomial over K of degree $2k$. Furthermore, Meyn [9] proved the following result.

Lemma 1.4 *([9, Theorem 6]). Let $f(X) = X^k + \cdots + a_1X + a_0 \in \mathbb{F}_{2^t}[X]$ be irreducible. Then $\Phi(f(X))$ is irreducible over $\mathbb{F}_{2^t}$ if and only if $a_0 \neq 0$ and $T_{2^t}(a_1/a_0) = 1$.*

The paper is organized as follows. In Section 2, we give some results on the existence and nonexistence of an elements $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$. Section 3 is a brief discussion of a connection of Question 1.1 with an open question by Wiedemann. In Section 4, we explore a connection of Question 1.1 with a game called "Button Madness" described by Blokhuis and Brouwer in [1]. The results of [1] provide answers to Question 1.1 with $j \leq 15$. Section 4 also contains a technical result about the absolute irreducibility of a certain bivariate polynomial in characteristic 2. Finally, we point out that $D_m(X)$ in Question 1.1 can be replaced by the so-called Dickson polynomial of the second kind of degree m with parameter 1 over $\mathbb{F}_q$ in Section 5.

2. Some existence and non-existence results

Recall that $q = 2^n$ with $n > 0$ and $m > 1$ is a divisor of $q+1$. (The case $m = 1$ is ignored since $D_1(X) = X$ has only one root 0.) Let $N_m = |\{\alpha \in \mathbb{F}_q^* : D_m(\alpha) = D_m(\alpha^{-1}) = 0\}|$. First, we consider the case $m = q+1$. Let χ_q be the canonical additive character of $\mathbb{F}_q$ defined by $\chi_q(x) = (-1)^{T_q(x)}$, $x \in \mathbb{F}_q$.

Theorem 2.1. *We have*

$$N_{q+1} = \frac{q+1+K(\chi_q)}{4},$$

where $K(\chi_q) = \sum_{x\in\mathbb{F}_q^*} \chi_q(x+x^{-1})$ is a Kloosterman sum.

Proof. For $\alpha \in \mathbb{F}_q^*$, let $f_\alpha(X) = X^2 + \alpha X + 1$. Then α is a root of $D_{q+1}(X)$ if and only if $f_\alpha(X)$ is irreducible over $\mathbb{F}_q$, i.e., if and only if $T_q(\alpha^{-1}) = 1$ (by Lemma 1.2). Hence, both α and α^{-1} are roots of $D_{q+1}(X)$ if and only if $T_q(\alpha^{-1}) = 1 = T_q(\alpha)$. Note that $T_q(\alpha) = 1$ if and only if $\chi_q(\alpha) = -1$. Therefore,

$$\begin{aligned} N_{q+1} &= \frac{1}{4}\sum_{\alpha\in\mathbb{F}_q^*}(1-\chi_q(\alpha))(1-\chi_q(\alpha^{-1})) \\ &= \frac{1}{4}\sum_{\alpha\in\mathbb{F}_q^*}\big(1-\chi_q(\alpha)-\chi_q(\alpha^{-1})+\chi_q(\alpha)\chi_q(\alpha^{-1})\big) \\ &= \frac{1}{4}\big(q-1+1+1+\sum_{\alpha\in\mathbb{F}_q^*}\chi_q(\alpha+\alpha^{-1})\big) \\ &= \frac{q+1+K(\chi_q)}{4}. \end{aligned}$$

In the above, we used the fact that $\sum_{\alpha\in\mathbb{F}_q^*}\chi_q(\alpha)=-1$. □

By [8, Theorem 5,43], it is easy to determine that

$$K(\chi_q) = -\frac{(-1+\sqrt{-7})^n+(-1-\sqrt{-7})^n}{2^n}. \tag{2}$$

By (2), or by [8, Theorem 5.45], $|K(\chi_q)|\le 2q^{1/2}$. Hence, it follows from Theorem 2.1 that $N_{q+1}\ge (q+1-2q^{1/2})/4>0$, i.e., there is always $\alpha\in\mathbb{F}_q^*$ so that both α and α^{-1} are roots of $D_{q+1}(X)$. On the other hand, when $q>4$, $K(\chi_q)\le 2q^{1/2}<q-1$, hence there exists $\alpha\in\mathbb{F}_q^*$ such that $T_q(\alpha)=1$ and $T_q(\alpha^{-1})=0$, i.e., α is a root of $D_{q+1}(X)$, but α^{-1} is not. For $q=2$, we have $\mathbb{F}_2^*=\{1\}$ and $1=1^{-1}$ is a root of $D_3(X)$. For $q=4$, we have that $\mathbb{F}_4^*=\{1,\zeta,\zeta^2\}$ with ζ a root of X^2+X+1 and $\alpha\in\mathbb{F}_q^*$ is a root of $D_5(X)$ if and only if either $\alpha=\zeta$ or $\alpha=\zeta^2$. We summarize these observations as follows.

Corollary 2.2. *Let n be a positive integer and $q=2^n$. There is $\alpha\in\mathbb{F}_q^*$ such that both α and α^{-1} are roots of $D_{q+1}(X)$. When $q>4$, there is $\alpha\in\mathbb{F}_q^*$ such that α is a root of $D_{q+1}(X)$, but α^{-1} is not. For $q=2,4$, there is no $\alpha\in\mathbb{F}_q^*$ such that α is a root of $D_{q+1}(X)$, but α^{-1} is not.*

In fact, Corollary 2.2 can be made slightly more general.

Theorem 2.3. *Let n be a positive integer and $q=2^n$. If $m=(2^k+1)\ell\mid(q+1)$ for some positive integers k and ℓ, then there is $\alpha\in\mathbb{F}_q^*$ such that both α and α^{-1} are roots of $D_m(X)$. Moreover, when $k>2$, there is $\alpha\in\mathbb{F}_q^*$ such that α is a root of $D_m(X)$, but α^{-1} is not.*

Proof. Since $(2^k+1)\mid(2^n+1)$, we have $k\mid n$ and n/k is odd. By Corollary 2.2, there is $\alpha\in\mathbb{F}_{2^k}^*$ such that both α and α^{-1} are roots of $D_{2^k+1}(X)$. It follows that α and α^{-1} are both roots of $D_m(X)=D_\ell(D_{2^k+1}(X))$.

Assume that $k>2$. By Corollary 2.2, there is $\alpha\in\mathbb{F}_{2^k}^*$ such that α is a root of $D_{2^k+1}(X)$, but α^{-1} is not. It follows that $D_m(\alpha)=0$. Since $D_{2^k+1}(\alpha^{-1})\ne 0$, $T_{2^k}(\alpha)=0$.

Hence $T_{2^n}(\alpha) = 0$, i.e., $D_{2^n+1}(\alpha^{-1}) \neq 0$. This implies $D_m(\alpha^{-1}) \neq 0$ since $D_m(\alpha^{-1}) = 0$ implies $D_{2^n+1}(\alpha^{-1}) = D_{(2^n+1)/m}(D_m(\alpha^{-1})) = D_{(2^n+1)/m}(0) = 0$. $\square$

Lemma 2.4. *Write $s = (q+1)/m$. Then the following statements are equivalent.*

(i) *There is $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$.*
(ii) *There are $x, y \in \mathbb{F}_{q^2}$ such that $x^m = 1 = y^m$ and $(x + x^q)(y + y^q) = 1$.*
(iii) *There are $x, y \in \mathbb{F}_{q^2}$ such that $x^{m(q-1)} = 1 = y^{m(q-1)}$, $x + x^q = 1 = y + y^q$, and $x^{q+1}y^{q+1} = 1$.*
(iv) *There are $x, y \in \mathbb{F}_{q^2}$ such that $x + x^q = 1 = y + y^q$ and*

$$\frac{(x^s + x^{qs})^2}{x^{(q+1)s}} \cdot \frac{(y^s + y^{qs})^2}{y^{(q+1)s}} = 1.$$

Proof. (i) $\Rightarrow$ (ii). Write $\alpha = x + x^{-1}$ and $\alpha^{-1} = y + y^{-1}$, where $x, y \in \mathbb{F}_{q^2}^*$. Since $D_m(\alpha) = D_m(\alpha^{-1}) = 0$, we have $x^m = 1 = y^m$ (and so $x^{q+1} = 1 = y^{q+1}$). Thus, $(x + x^q)(y + y^q) = (x + x^{-1})(y + y^{-1}) = \alpha\alpha^{-1} = 1$.

(ii) $\Rightarrow$ (iii). Let

$$x_1 = \frac{x}{x + x^q}, \quad y_1 = \frac{y}{y + y^q}.$$

Then the conditions in (iii) are satisfied by x_1 and y_1.

(iii) $\Rightarrow$ (iv). Since $x^{m(q-1)} = 1 = y^{m(q-1)}$ and $x + x^q = 1 = y + y^q$, there exist $x_1, y_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $x = x_1^s$ and $y = y_1^s$. Let

$$x_2 = \frac{x_1}{x_1 + x_1^q}, \quad y_2 = \frac{y_1}{y_1 + y_1^q}.$$

Then the conditions in (iv) are satisfied by x_2 and y_2. Indeed, $x_2 + x_2^q = 1 = y_2 + y_2^q$ and moreover,

$$\begin{aligned}\frac{(x_2^s + x_2^{qs})^2}{x_2^{(q+1)s}} \cdot \frac{(y_2^s + y_2^{qs})^2}{y_2^{(q+1)s}} &= \frac{(x_1^s + x_1^{qs})^2}{(x_1 + x_1^q)^{2s}} \Big(\frac{x_1 + x_1^q}{x_1}\Big)^{(q+1)s} \frac{(y_1^s + y_1^{qs})^2}{(y_1 + y_1^q)^{2s}} \Big(\frac{y_1 + y_1^q}{y_1}\Big)^{(q+1)s} \\ &= \frac{(x + x^q)^2 (y + y^q)^2}{x^{q+1} y^{q+1}} = 1.\end{aligned}$$

(iv) $\Rightarrow$ (i). Let $x_1 = x^{(q-1)s}$ and $y_1 = y^{(q-1)s}$. Clearly, $x_1^m = 1 = y_1^m$, and

$$\begin{aligned}(x_1 + x_1^q)(y_1 + y_1^q) &= (x^{(q-1)s} + x^{(1-q)s})(y^{(q-1)s} + y^{(1-q)s}) \\ &= x^{-(q+1)s}(x^{2s} + x^{2qs}) y^{-(q+1)s}(y^{2s} + y^{2qs}) \\ &= \frac{(x^s + x^{qs})^2}{x^{(q+1)s}} \cdot \frac{(y^s + y^{qs})^2}{y^{(q+1)s}} = 1.\end{aligned}$$

Letting $\alpha = x_1 + x_1^q$, we have $\alpha^{-1} = y_1 + y_1^q$ and $D_m(\alpha) = D_m(\alpha^{-1}) = 0$. $\square$

Remark 2.5. Concerning statement (iii) of Lemma 2.4, a direct computation shows that there are precisely $m-1$ elements $x \in \mathbb{F}_{q^2}$ such that $x^{m(q-1)} = 1$ and $x + x^q = 1$.

For α in the algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$, let $m_\alpha(X)$ denote the minimal polynomial of α over $\mathbb{F}_2$.

Lemma 2.6. *Let $f(X) \in \mathbb{F}_2[X]$ be irreducible such that $f(0) \neq 0$ and $\Phi(f(X)) \mid (X^{q+1} + 1)$. Then $\Phi(f(X))$ is irreducible over $\mathbb{F}_2$.*

Proof. Let $0 \neq \alpha \in \overline{\mathbb{F}}_2$ be a root of $f(X)$ and write $\alpha = \zeta + \zeta^{-1}$, where $0 \neq \zeta \in \overline{\mathbb{F}}_2$. Then ζ is a root of $\Phi(f(X))$, and hence $\zeta^{q+1} = 1$. It follows that $\alpha \in \mathbb{F}_q$. Since $\zeta^q = \zeta^{-1} \neq 1$, we have $\zeta \notin \mathbb{F}_q$, in particular, $\zeta \notin \mathbb{F}_2(\alpha)$. Thus $[\mathbb{F}_2(\zeta) : \mathbb{F}_2(\alpha)] = 2$. Since $[\mathbb{F}_2(\zeta) : \mathbb{F}_2] = [\mathbb{F}_2(\zeta) : \mathbb{F}_2(\alpha)][\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2 \deg f = \deg \Phi(f(X))$, we have $\Phi(f(X)) = m_\zeta(X)$, which is irreducible over $\mathbb{F}_2$. $\square$

Lemma 2.7. *Let $q = 2^n$ and m be a divisor of $q+1$. Then there is an element $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$ if and only if $X^m + 1$ has a self-reciprocal polynomial factor of the form $\Phi(f(X)) = X^{\deg f} f(X + X^{-1})$, where $f(X) \in \mathbb{F}_2[X]$ is either self-reciprocal and irreducible or is a product of two different irreducible polynomials over $\mathbb{F}_2$ which are reciprocals of each other.*

Remark 2.8. Assume that $f(X) \in \mathbb{F}_2[X]$ is such that $\Phi(f(X)) \mid (X^m+1)$. By Lemma 2.6, if $f(X) \in \mathbb{F}_2[X]$ is self-reciprocal and irreducible, $\Phi(f(X)) \in \mathbb{F}_2[X]$ is irreducible; if $f(X)$ is a product of a reciprocal pair of irreducible polynomials $f_1(X)$ and $f_2(X)$ over $\mathbb{F}_2$, then $\Phi(f(x)) = \Phi(f_1(X))\Phi(f_2(X))$, where $\Phi(f_1(X))$ and $\Phi(f_2(X))$ are irreducible over $\mathbb{F}_2$ by Lemma 2.6 again.

Proof of Lemma 2.7. ($\Rightarrow$) Write $\alpha = \zeta + \zeta^{-1}$ and $\alpha^{-1} = \lambda + \lambda^{-1}$, where $\zeta, \lambda \in \overline{\mathbb{F}}_2^*$. Since $D_m(\alpha) = 0$, we know that $\zeta^m = 1$ and $X^2 + \alpha X + 1$ is the minimal polynomial of ζ over $\mathbb{F}_2(\alpha)$. Note that ζ is a root of $\Phi(m_\alpha(X)) = X^{\deg m_\alpha} m_\alpha(X + X^{-1})$. Since $[\mathbb{F}_2(\zeta) : \mathbb{F}_2] = [\mathbb{F}_2(\zeta) : \mathbb{F}_2(\alpha)][\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2 \deg m_\alpha = \deg \Phi(m_\alpha(X))$, we have $m_\zeta(X) = \Phi(m_\alpha(X))$. In the same way, $\lambda^m = 1$ and $m_\lambda(X) = \Phi(m_{\alpha^{-1}}(X))$.

If α and α^{-1} are conjugate over $\mathbb{F}_2$, then $m_\alpha(X)$ is self-reciprocal and $\Phi(m_\alpha(X)) \mid (X^m + 1)$.

If α and α^{-1} are not conjugate over $\mathbb{F}_2$, then $m_\alpha(X)$ and $m_{\alpha^{-1}}(X)$ are not self-reciprocal but are reciprocals of each other. Clearly, ζ and λ are not conjugate over $\mathbb{F}_2$. Hence $m_\zeta(X) \neq m_\lambda(X)$ and consequently, $\Phi(m_\alpha(X) m_{\alpha^{-1}}(X)) = m_\zeta(X) m_\lambda(X) \mid (X^m + 1)$.

($\Leftarrow$) By assumption, $\Phi(f(X)) \mid (X^m + 1)$ for some self-reciprocal $f(X) \in \mathbb{F}_2[X]$ with $\deg f > 0$. Let α be any root of $f(X)$ and write $\alpha = \zeta + \zeta^{-1}$, where $\alpha, \zeta \in \overline{\mathbb{F}}_2^*$. Then ζ is a root of $\Phi(f(X))$ and hence $\zeta^m = 1$. Then $\alpha \in \mathbb{F}_q$ (since $m \mid (q+1)$), and $D_m(\alpha) = 0$. Since α^{-1} is also a root of $f(X)$, we have $D_m(\alpha^{-1}) = 0$. $\square$

Corollary 2.9. *Suppose that $m \mid q+1$ and let*

$$\frac{X^m+1}{X+1} = f_1(X)f_1^*(X)\cdots f_r(X)f_r^*(X)b_1(X)\cdots b_s(X)$$

be the factorization of $(X^m+1)/(X+1)$ over $\mathbb{F}_2$, where $f_i(X)$ and $f_i^*(X)$, $1 \le i \le r$, are reciprocal pairs of irreducible polynomials, and $b_j(X)$, $1 \le j \le s$, are self-reciprocal irreducible polynomials. Then there is no $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$ if one of the following holds:

(i) *$s = 0$;*
(ii) *$s \ge 1$ and for each $1 \le j \le s$, the coefficient of $X^{\deg(b_j(X))-1}$ in $b_j(X)$ is zero.*

Proof. Assume to the contrary that there exists $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$. By Lemma 2.7 and Remark 2.8, $s \ge 1$ and we may assume that $b_1(X) = \Phi(f^*(X))$ for some irreducible $f(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0 \in \mathbb{F}_2[X]$. Since $b_1(X)$ is irreducible over $\mathbb{F}_2$, by Lemma 1.4, $a_0 = a_1 = 1$. Hence

$$\begin{aligned}\Phi(f^*(X)) &= X^k\big((X+X^{-1})^k + (X+X^{-1})^{k-1} + \cdots + a_{k-1}(X+X^{-1}) + 1\big)\\ &= X^{2k} + X^{2k-1} + \cdots,\end{aligned}$$

whose coefficient of X^{2k-1} is 1. This is a contradiction. □

Theorem 2.10. *Let $q = 2^n$ and let $m > 3$ be a prime divisor of $q+1$ such that $m \equiv 3 \pmod 4$. If 2 is a primitive element of $\mathbb{F}_m$, i.e., the order of 2 in $\mathbb{F}_m^*$ is $m-1$, then there is no element $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$.*

Proof. Assume to the contrary that there exists $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$. Since 2 is a primitive element of $\mathbb{F}_m$, it follows from [8, Theorem 2.47] that $(X^m+1)/(X+1)$ is irreducible over $\mathbb{F}_2$. By Lemma 2.7, $(X^m+1)/(X+1) = \Phi(f(X))$ for some self-reciprocal irreducible polynomial $f(X)$ over $\mathbb{F}_2$. Since $\deg f = \frac{1}{2}\deg\Phi(f(X)) = \frac{1}{2}(m-1) \ge 2$, the irreducibility and self-reciprocity of f imply that $\deg f$ is even. This is a contradiction since $m \equiv 3 \pmod 4$. □

Remark 2.11. A special case of Artin's conjecture on primitive roots states that there are infinitely many primes p such that 2 is a primitive element of $\mathbb{F}_p$. The set of such primes is Sequence A001122 in OEIS [10].

Proposition 2.12. *Suppose that $q = 2^n$ with $n \ge 3$ and that $m > 5$ is a divisor of $q+1$. Then there is $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = 0$ but $D_m(\alpha^{-1}) \ne 0$.*

Proof. Write $\alpha = \zeta + \zeta^{-1}$. Then α is a root of $D_m(X)$ if and only if ζ is a root of X^m+1. Since $m|(q+1)$, every root ζ of X^m+1 satisfies $\zeta^{q+1} = 1$, and so $\zeta \in \mathbb{F}_{q^2}$. This implies

that $\alpha^q = (\zeta + \zeta^{-1})^q = \zeta + \zeta^{-1} = \alpha$, i.e., $\alpha \in \mathbb{F}_q$. Hence, every root of $D_m(X)$ belongs to $\mathbb{F}_q$.

Write

$$f(X) = \sum_{i=0}^{\frac{m-1}{2}} \frac{m}{m-i}\binom{m-i}{i} X^{(m-2i-1)/2}.$$

Then, $D_m(X) = Xf(X)^2$ by the definition of Dickson polynomial. So, $\alpha \in \mathbb{F}_q^*$ is a root of $D_m(X)$ if and only if α is a root of $f(X)$. This implies that $\alpha = \zeta + \zeta^{-1} \in \mathbb{F}_q^*$ is a root of $f(X)$ if and only if ζ is a root of $\frac{X^m+1}{X+1}$. Since $\frac{X^m+1}{X+1}$ is simple, it is easy to see that $\frac{X^m+1}{X+1} = \Phi(f(X))$ and so, $f(X)$ is simple. Moreover, if every root $\alpha \in \mathbb{F}_q^*$ of $D_m(X)$ satisfies $D_m(\alpha^{-1}) = 0$, then every root α of $f(X)$ satisfies $f(\alpha^{-1}) = 0$. This implies that $f(X)$ must be a self-reciprocal polynomial. So, if we can show that $f(X)$ is not self-reciprocal, then we are done.

Also write $f(X) = \sum_{i=0}^{\frac{m-1}{2}} a_i X^i$. Then $a_{\frac{m-1}{2}} = \frac{m}{m-0}\binom{m-0}{0} \equiv 1 \mod 2$, $a_{\frac{m-3}{2}} = \frac{m}{m-1}\binom{m-1}{1} \equiv 1 \mod 2$, $a_0 = \frac{m}{m-(m-1)/2}\binom{m-(m-1)/2}{(m-1)/2} = \frac{m}{(m+1)/2}\binom{(m+1)/2}{1} \equiv 1 \mod 2$, and $a_1 = \frac{m}{(m+3)/2}\binom{(m+3)/2}{3}$. Note that $a_1 \equiv 0 \mod 2$ when $m \equiv \pm 1 \mod 8$ and $a_1 \equiv 1 \mod 2$ when $m \equiv \pm 3 \mod 8$. So, if $m \equiv \pm 1 \mod 8$, then $f(X)$ is not self-reciprocal.

From now on, let $m \equiv \pm 3 \mod 8$. We already have $a_{\frac{m-1}{2}} = a_{\frac{m-3}{2}} = a_1 = a_0 = 1$. Since $m > 5$, we have $m \geq 11$ and so we can consider $a_{\frac{m-5}{2}}$ and a_2. $a_{\frac{m-5}{2}} = \frac{m}{m-2}\binom{m-2}{2} \equiv 1 \mod 2$ if $m \equiv -3 \mod 8$, and $a_{\frac{m-5}{2}} = \frac{m}{m-2}\binom{m-2}{2} \equiv 0 \mod 2$ if $m \equiv 3 \mod 8$. $a_2 = \frac{m}{m-(m-5)/2}\binom{m-(m-5)/2}{(m-5)/2} \equiv 0$ if $m \equiv 13 \mod 16$, and $a_2 \equiv 1$ if $m \equiv 11 \mod 16$. Hence, $f(X)$ is not self-reciprocal if $m \equiv 11, 13 \mod 16$. The remaining cases are $m \equiv 3, 5 \mod 16$.

For $m \equiv 3 \mod 16$, we have that $m \geq 19$, and that $a_{\frac{m-7}{2}} = \frac{m}{m-3}\binom{m-3}{3} \equiv 1 \mod 2$ and $a_3 = \frac{m}{m-(m-7)/2}\binom{m-(m-7)/2}{(m-7)/2} \equiv 0 \mod 2$. For $m \equiv 5 \mod 16$, we have that $m \geq 21$, and that $a_{\frac{m-9}{2}} = \frac{m}{m-4}\binom{m-4}{4} \equiv 0 \mod 2$, and $a_4 = \frac{m}{m-(m-9)/2}\binom{m-(m-9)/2}{(m-9)/2} \equiv 1 \mod 2$ if $m \equiv 21 \mod 32$. Finally, for $m \equiv 5 \mod 32$, we have that $m \geq 37$, and that $a_{\frac{m-11}{2}} = \frac{m}{m-5}\binom{m-5}{5} \equiv 1 \mod 2$ and $a_5 = \frac{m}{m-(m-11)/2}\binom{m-(m-11)/2}{(m-11)/2} \equiv 0 \mod 2$. All of these imply that $f(X)$ is not self-reciprocal when $m \equiv 3, 5 \mod 16$. $\square$

3. A connection to Wiedemann's question

In [11], Wiedemann considered a sequence $x_j \in \overline{\mathbb{F}}_2$, $j \geq -1$, defined recursively by

$$\begin{cases} x_{-1} = 1, \\ x_{j+1} + x_{j+1}^{-1} = x_j, \quad j \geq -1. \end{cases} \tag{3}$$

It was proved in [11] that for $j \geq 0$, $\mathbb{F}_2(x_j) = \mathbb{F}_{2^{2^{j+1}}}$ and $x_j^{F_j} = 1$, where $F_j = 2^{2^j} + 1$ is the jth Fermat number. Wiedemann raised the following question which is still unsolved:

Is $x_0x_1\cdots x_n$ a primitive element of $\mathbb{F}_{2^{2^{n+1}}}$ for all $n \geq 0$? Since the Fermat numbers are pairwise relatively prime [5, Theorem 16] and $F_0F_1\cdots F_n = 2^{2^{n+1}}-1$, the above question is equivalent to the following

Question 3.1 *(Wiedemann).* Let x_j be defined by (3) and let $o(x_i)$ denote its multiplicative order. For each $j \geq 0$, is it true that $o(x_j) = F_j$?

Our computational results confirm a positive answer to Question 3.1 for $0 \leq j \leq 11$ and provide partial evidence for a positive answer for $j = 12$ and 13. For $0 \leq j \leq 4$, F_j is a prime, and hence $o(x_j) = F_j$. For $5 \leq j \leq 11$, the complete factorization of F_j is known [12]. We have verified that for each prime factor d of F_j $(5 \leq j \leq 11)$, $x_j^{F_j/d} \neq 1$, and hence $o(x_j) = F_j$. For $j = 12$ and 13, only partial factorizations of F_{12} and F_{13} are known [12]:

$$F_{12} = p_6 \cdot p_8 \cdot p'_8 \cdot p_{12} \cdot p_{16} \cdot p_{54} \cdot c_{1133},$$
$$F_{13} = p_{13} \cdot p_{19} \cdot p'_{19} \cdot p_{27} \cdot c_{2391},$$

where p_i (p'_i) is a known prime with i digits and c_i is a known composite number with i digits. We have verified that

$$x_{12}^{F_{12}/d} \neq 1 \quad \text{for } d \in \{p_6, p_8, p'_8, p_{12}, p_{16}, p_{54}, c_{1133}\}$$

and

$$x_{13}^{F_{13}/d} \neq 1 \quad \text{for } d \in \{p_{13}, p_{19}, p'_{19}, p_{27}, c_{2391}\}.$$

The question that we consider in the present paper is related to Question 3.1 in the following sense. Let $o(x_j) = m_j$. Also write $x_{j-1}^{-1} = y_j + y_j^{-1}$, where $y_j \in \mathbb{F}_{2^{2^{j+1}}}$. Since x_{j-1} and x_{j-1}^{-1} are conjugate over $\mathbb{F}_{2^{2^{j-1}}}$ in Wiedemann's construction, we have that y_j is conjugate to either x_j or x_j^{-1} over $\mathbb{F}_{2^{2^{j-1}}}$, and so $o(y_j) = m_j$. Then $x_j^{m_j} = y_j^{m_j} = 1$ and $(x_j + x_j^{-1})(y_j + y_j^{-1}) = 1$; that is, $D_{m_j}(x_{j-1}) = D_{m_j}(x_{j-1}^{-1}) = 0$. If for every proper divisor m of F_j, there is no $\alpha \in \mathbb{F}^*_{2^{2^j}}$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$, then $o(x_j) = F_j$. Therefore, it is natural to ask the following question, which is a restatement of Question 1.1 for a given j.

Question 3.2. Let $j \geq 0$ be an integer. Do there exist a proper divisor m of F_j and $\alpha \in \mathbb{F}^*_{2^{2^j}}$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$?

The answer to Question 3.2 is negative for $0 \leq j \leq 4$ and is positive for $j = 5$ and $8 \leq j \leq 15$; see Section 4.

4. A connection to mad numbers

In [1], Blokhuis and Brouwer described a game as following: Let m be a positive integer and let Γ_m be the graph with vertex set $\mathbb{Z}_m \times \mathbb{Z}_m$ such that $(x_1, x_2), (y_1, y_2) \in \mathbb{Z}_m \times \mathbb{Z}_m$ are adjacent if and only if either $x_1 = y_1$, $x_2 - y_2 \equiv \pm 1 \mod m$ or $x_1 - y_1 \equiv \pm 1 \mod m$, $x_2 = y_2$. Each vertex of Γ_m is of valency 4 and equipped with a light bulb and a button. Pushing the button at a vertex x switches the state (light on/off) of x and each of its neighbors. If there exist nonempty sets of buttons such that pushing all of them does leave the starting state pattern unchanged, Blokhuis and Brouwer call the number m *mad*.

Let the vertex $(u, v) \in \mathbb{Z}_m \times \mathbb{Z}_m$ correspond to the monomial $X^u Y^v \in \mathbb{F}_2[X, Y]/(X^m - 1, Y^m - 1)$. Each given state pattern corresponds to a polynomial $f(X, Y) \in \mathbb{F}_2[X, Y]/(X^m - 1, Y^m - 1)$. Let

$$i(X, Y) = 1 + X + X^{-1} + Y + Y^{-1} \in \mathbb{F}_2(X, Y).$$

Pushing a button at (u, v) means adding $i(X, Y)X^u Y^v$ to $f(X, Y)$. So, m is mad if and only if there is a nonzero polynomial $g(X, Y) \in \mathbb{F}_2[X, Y]/(X^m - 1, Y^m - 1)$ so that $g(X, Y)i(X, Y) = 0$ in $\mathbb{F}_2[X, Y]/(X^m - 1, Y^m - 1)$, or equivalently, $(i(X, Y))$ is a proper ideal in $\mathbb{F}_2[X, Y]/(X^m - 1, Y^m - 1)$ (see [1]). It was proved in [1] that m is mad if and only if there exist $x, y \in \overline{\mathbb{F}}_2$ with $x^m = y^m = 1$ such that $i(x, y) = 0$.

Let

$$\mathcal{A}_m = \left\{(x, y) \in \overline{\mathbb{F}}_2 : x^m = y^m = 1,\ (x + x^{-1})(y + y^{-1}) = 1\right\},$$
$$\mathcal{B}_m = \left\{(x, y) \in \overline{\mathbb{F}}_2 : x^m = y^m = 1,\ i(x, y) = 0\right\}.$$

The map $\mathcal{A}_m \to \mathcal{B}_m$, $(x, y) \mapsto (xy, xy^{-1})$ is a bijection whose inverse is $(x, y) \mapsto ((xy)^{1/2}, (xy^{-1})^{1/2})$. Hence $|\mathcal{A}_m| = |\mathcal{B}_m|$. Assume that $m \mid (q + 1)$ and let

$$\mathcal{D}_{m,q} = \left\{\alpha \in \mathbb{F}_q^* : D_m(\alpha) = D_m(\alpha^{-1}) = 0\right\}.$$

Recall that the map $\mathcal{A}_m \to \mathcal{D}_{m,q}$, $(x, y) \mapsto x + x^{-1}$, is a 4-to-1 onto map, and hence $|\mathcal{D}_{m,q}| = \frac{1}{4}|\mathcal{A}_m| = \frac{1}{4}|\mathcal{B}_m|$. In particular, there exists $\alpha \in \mathbb{F}_q^*$ such that $D_m(\alpha) = D_m(\alpha^{-1}) = 0$ if and only if m is a mad number. Therefore, Question 3.2 can be rephrased as follows:

Question 4.1. Does the Fermat number F_j have any proper divisor that is a mad number?

For $0 \le j \le 4$, F_j are primes, and hence the answer to Question 4.1 is negative. For $j = 5$, the numerical results of [1] indicate that the prime divisor 6700417 of F_5 is mad but the other prime divisor 641 is not. Hence the answer to Question 4.1 is positive for $j = 5$. More importantly, the following theorem of [1] shows that large divisors of F_j are mad.

Table 1
Values of $\log_{10} a(j)$ and $(2^{j-2}-2)\log_{10} 2$, $5 \le j \le 15$.

j	$\log_{10} a(j)$	$(2^{j-2}-2)\log_{10} 2$
5	2.80686	1.80618
6	5.43803	4.21442
7	16.7756	9.0309
8	15.093	18.6639
9	6.38468	37.9298
10	7.65889	76.4616
11	5.50446	153.525
12	5.05952	307.653
13	12.4331	615.907
14	53.0679	1232.42
15	9.08431	2465.44

Theorem 4.2 *([1]). If $d \mid (2^k+1)$ is such that $(4d)^4 \le 2^k$, then $(2^k+1)/d$ is a mad number.*

Let $a(j)$ denote the smallest prime divisor of F_j; this is Sequence A093179 in OEIS where $a(j)$ are listed for $0 \le j \le 15$. If

$$\log_{10} a(j) \le (2^{j-2}-2)\log_{10} 2, \tag{4}$$

then by Theorem 4.2, $F_j/a(j)$ is a mad number. The (approximate) values of $\log_{10} a(j)$ and $(2^{j-2}-2)\log_{10} 2$, $5 \le j \le 15$, are given in Table 1.

For $8 \le j \le 15$, (4) is satisfied, hence for these values of j, $F_j/a(j)$ is mad and the answer to Question 4.1 is positive.

The proof of Theorem 4.2 provided in [1] relies on the Hasse–Weil bound applied to a certain polynomial $H(U,V) \in \mathbb{F}_{2^k}[U,V]$ (defined below). To this end, the polynomial $H(U,V)$ needs to be absolutely irreducible. However, the proof in [1] does not include a verification or explanation for the absolute irreducibility of $H(U,V)$. It appears to us that the absolute irreducibility of $H(U,V)$ is nontrivial and it took us much effort to prove this fact. For the sake of completeness, we include a proof of the absolute irreducibility of $H(U,V)$ and a more detailed proof of Theorem 4.2.

Proposition 4.3. *Let $d > 0$ be odd and $0 \ne a \in \overline{\mathbb{F}}_2$. Define*

$$H(U,V) = (U^2+U+a)^d(V^2+V+a)^d\Big[1+D_d\Big(\frac{1}{U^2+U+a}\Big)+D_d\Big(\frac{1}{V^2+V+a}\Big)\Big]. \tag{5}$$

Then H is irreducible in $\overline{\mathbb{F}}_2[U,V]$.

Proof. 1° We claim that $1+D_d(X)+D_d(Y) \in \overline{\mathbb{F}}_2[X,Y]$ is irreducible.

First, note that $\deg D_d = d$, and since d is odd, we can write $D_d(X) = Xf_d(X^2)$ for some monic polynomial $f_d \in \overline{\mathbb{F}}_2[X]$ with $\deg f_d = (d-1)/2$. The homogenization of $1+D_d(X)+D_d(Y)$ is

$$F(X,Y,Z) = Z^d + XZ^{d-1} f_d\Big(\Big(\frac{X}{Z}\Big)^2\Big) + YZ^{d-1} f_d\Big(\Big(\frac{Y}{Z}\Big)^2\Big) \in \overline{\mathbb{F}}_2[X,Y,Z].$$

It suffices to show that the projective curve F is smooth, i.e., without singular point in the projective plane $\mathbb{P}^2(\overline{\mathbb{F}}_2)$. (If F is smooth, it is irreducible over $\overline{\mathbb{F}}_2$. It follows that $1 + D_d(X) + D_d(Y)$ is irreducible in $\overline{\mathbb{F}}_2[X,Y]$.) We have

$$\begin{aligned}
\frac{\partial F}{\partial X} &= Z^{d-1} f_d\Big(\Big(\frac{X}{Z}\Big)^2\Big),\\
\frac{\partial F}{\partial Y} &= Z^{d-1} f_d\Big(\Big(\frac{Y}{Z}\Big)^2\Big),\\
\frac{\partial F}{\partial Z} &= Z^{d-1}.
\end{aligned}$$

Assume to the contrary that F has a singular point $P = (x : y : z) \in \mathbb{P}^2(\overline{\mathbb{F}}_2)$, i.e.,

$$F(P) = \frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Then $z = 0$. Since

$$\begin{aligned}
\frac{\partial F}{\partial X} &= Z^{d-1} f_d\Big(\Big(\frac{X}{Z}\Big)^2\Big) = Z^{d-1}\Big(\Big(\frac{X}{Z}\Big)^{d-1} + \text{lower terms in } \frac{X}{Z}\Big)\\
&= X^{d-1} + Z\cdot(\cdots),
\end{aligned}$$

it follows from $(\partial F/\partial X)(P) = 0$ that $x = 0$. In the same way, $y = 0$. Thus we have a contradiction.

2° Let x, y, u, v be transcendentals over $\overline{\mathbb{F}}_2$ such that $1+D_d(x)+D_d(y) = 0$, $u^2+u+a = x^{-1}$ and $v^2 + v + a = y^{-1}$. We claim that

$$[\overline{\mathbb{F}}_2(y,u) : \overline{\mathbb{F}}_2(y)] = 2d.$$

First, we have $[\overline{\mathbb{F}}_2(u) : \overline{\mathbb{F}}_2(x)] = 2$. Otherwise, $u \in \overline{\mathbb{F}}_2(x)$. Write $u = f(x^{-1})/g(x^{-1})$, where $f, g \in \overline{\mathbb{F}}_2[X]$ satisfy $\gcd(f,g) = 1$. Then

$$\Big(\frac{f(x^{-1})}{g(x^{-1})}\Big)^2 + \frac{f(x^{-1})}{g(x^{-1})} + a = x^{-1}.$$

Since x is transcendental over $\overline{\mathbb{F}}_2$, we have

$$\Big(\frac{f}{g}\Big)^2 + \frac{f}{g} + a = X,$$

i.e.,

$$(X + a)g^2 = f(f + g).$$

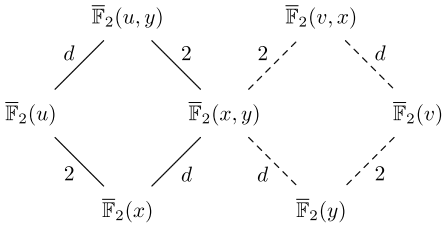

Fig. 1. Proof of Proposition 4.3.

Since $\gcd(g, f(f+g)) = 1$, we have $g = 1$. It follows that $X + a = f(f+1)$, which is impossible.

By 1°, $[\overline{\mathbb{F}}_2(x,y) : \overline{\mathbb{F}}_2(x)] = [\overline{\mathbb{F}}_2(x,y) : \overline{\mathbb{F}}_2(y)] = d$. Since $\gcd(2,d) = 1$, we have the solid part of the diagram in Fig. 1. (The dashed part follows by symmetry.)

3° We claim that $X^2 + X + x^{-1} + y^{-1} \in \overline{\mathbb{F}}_2(x,y)[X]$ is irreducible over $\overline{\mathbb{F}}_2(x,y)$.

Consider the function field $\overline{\mathbb{F}}_2(x,y)/\overline{\mathbb{F}}_2$. Let $(x)_0$ denote the zero divisor of x. Then

$$\deg(x)_0 = [\overline{\mathbb{F}}_2(x,y) : \overline{\mathbb{F}}_2(x)] = d.$$

Since d is odd, there is a place P of $\overline{\mathbb{F}}_2(x,y)$ such that $\nu_P(x) = k$ is a positive odd integer, where ν_P is the valuation at P. Then $\nu_P(D_d(x)) = \nu_P(xf_d(x^2)) > 0$. It follows from

$$1 + D_d(x) + D_d(y) = 0$$

that $\nu_P(D_d(y)) = 0$. Hence $\nu_P(y) = 0$. Therefore,

$$\nu_P(x^{-1} + y^{-1}) = -k.$$

Assume to the contrary that $X^2 + X + x^{-1} + y^{-1}$ has a root $\epsilon \in \overline{\mathbb{F}}_2(x,y)$. Then

$$\epsilon(\epsilon + 1) = x^{-1} + y^{-1}.$$

If $\nu_P(\epsilon) \geq 0$, then $\nu_P(\epsilon(\epsilon+1)) \geq 0$, which is a contradiction. If $\nu_P(\epsilon) < 0$, then $\nu_P(\epsilon(\epsilon+1)) = 2\nu_P(\epsilon)$, which is also impossible since $\nu_P(x^{-1} + y^{-1}) = -k$ is odd.

4° We claim that $[\overline{\mathbb{F}}_2(u,v) : \overline{\mathbb{F}}_2(u)] = 2d$. (By symmetry, $[\overline{\mathbb{F}}_2(u,v) : \overline{\mathbb{F}}_2(v)] = 2d$.)

Consider the following diagram.

$$\begin{array}{c}
\overline{\mathbb{F}}_2(u,v) \\
\Big| \ \leq 2 \\
\overline{\mathbb{F}}_2(u,y) \\
\Big| \ d \text{ (by Fig. 1)} \\
\overline{\mathbb{F}}_2(u)
\end{array}$$

Assume to the contrary that $v \in \overline{\mathbb{F}}_2(u, y) = \overline{\mathbb{F}}_2(u, x, y)$. Then

$$v = a_0(x, y) + ua_1(x, y) \tag{6}$$

for some $a_0, a_1 \in \overline{\mathbb{F}}_2(X, Y)$. Then

$$v^2 = a_0(x, y)^2 + u^2 a_1(x, y)^2. \tag{7}$$

Adding (6) and (7) gives

$$\begin{aligned} a + y^{-1} &= a_0(x, y) + a_0(x, y)^2 + ua_1(x, y) + u^2 a_1(x, y)^2 \\ &= a_0(x, y) + a_0(x, y)^2 + ua_1(x, y) + (u + a + x^{-1})a_1(x, y)^2 \\ &= a_0(x, y) + a_0(x, y)^2 + ua_1(x, y)(a_1(x, y) + 1) + (a + x^{-1})a_1(x, y)^2. \end{aligned}$$

We must have $a_1(x, y)(a_1(x, y)+1) = 0$. Otherwise, $u \in \overline{\mathbb{F}}_2(x, y)$, which is a contradiction to the diagram in Fig. 1.

If $a_1(x, y) = 0$, then $v = a_0(x, y) \in \overline{\mathbb{F}}_2(x, y)$, which is a contradiction to Fig. 1. Thus $a_1(x, y) = 1$. Hence

$$a_0(x, y)^2 + a_0(x, y) + x^{-1} + y^{-1} = 0.$$

However, this is impossible by 3°.

5°. We have $H(u, v) = 0$, where H is defined in (5). Note that $\deg_U H(U, V) = \deg_V H(U, V) = 2d$. By 4°, $H(U, v)$ is the minimal polynomial of u over $\overline{\mathbb{F}}_2(v)$. Hence $H(U, v)$ is irreducible over $\overline{\mathbb{F}}_2(v)$; that is, $H(U, V)$ is irreducible over $\overline{\mathbb{F}}_2(V)$. Write

$$H(U, V) = b_{2d}(V)U^{2d} + \cdots + b_0(V),$$

where $b_i(V) \in \overline{\mathbb{F}}_2[V]$, $\deg b_i \leq 2d$. Let

$$h(V) = \gcd(b_{2d}(V), \ldots, b_0(V)).$$

We claim that $h(V) = 1$. (Then it follows that $H(U, V)$ is irreducible over $\overline{\mathbb{F}}_2$.) Otherwise,

$$0 = H(u, v) = h(v)\frac{H(u, v)}{h(v)},$$

where $h(v) \neq 0$ since v is transcendental over $\overline{\mathbb{F}}_2$. Therefore $H(u, v)/h(v) = 0$. Thus v is of degree $< 2d$ over $\overline{\mathbb{F}}_2(u)$, which is a contradiction to 4°. □

The following result shows the equivalence of mad number and the existence of roots of the function $H(U, V)$.

Lemma 4.4. *Let d be a proper divisor of 2^k+1 and let $m=(2^k+1)/d$. Choose $a\in\mathbb{F}_{2^k}$ such that $T_{2^k}(a)=1$. Let*

$$H(U,V)=(U^2+U+a)^d(V^2+V+a)^d\Big[1+D_d\Big(\frac{1}{U^2+U+a}\Big)+D_d\Big(\frac{1}{V^2+V+a}\Big)\Big].$$

Then m is a mad number if and only if $H(U,V)$ has a root $(u,v)\in\mathbb{F}_{2^k}^2$.

Proof. We first assume that m is mad. Then there are $\alpha,\beta\in\mathbb{F}_{2^{2k}}$ so that

$$1+\alpha+\alpha^{-1}+\beta+\beta^{-1}=0 \text{ and } \alpha^m=1=\beta^m.$$

From $2^k+1=md$, $\alpha^m=1=\beta^m$ if and only if $\alpha=\xi^d$ and $\beta=\zeta^d$ for $\xi,\zeta\in\mathbb{F}_{2^{2k}}$ satisfying $\xi^{2^k+1}=1=\zeta^{2^k+1}$. In this situation, both $x=\xi+\xi^{-1}$ and $y=\zeta+\zeta^{-1}$ are in $\mathbb{F}_{2^k}$, and both X^2+xX+1 and X^2+yX+1 are irreducible over $\mathbb{F}_{2^k}$. Hence $T_{2^k}(x^{-1})=1=T_{2^k}(y^{-1})$. Not that every element in $\mathbb{F}_{2^k}$ of trace 1 is of the form b^2+b+a with $b\in\mathbb{F}_{2^k}$ as we have chosen $a\in\mathbb{F}_{2^k}$ with $T_{2^k}(a)=1$. So, $x^{-1}=u^2+u+a$ and $y^{-1}=v^2+v+a$ for some $u,v\in\mathbb{F}_{2^k}$. Thus,

$$\begin{aligned}0&=1+\alpha+\alpha^{-1}+\beta+\beta^{-1}\\&=1+\xi^d+(\xi^{-1})^d+\zeta^d+(\zeta^{-1})^d\\&=1+D_d(x)+D_d(y)\\&=1+D_d(\frac{1}{u^2+u+a})+D_d(\frac{1}{v^2+v+a}).\end{aligned}$$

It follows that $H(u,v)=0$.

Conversely, suppose that $H(U,V)$ has a root $(u,v)\in\mathbb{F}_{2^k}^2$. Since $T_{2^k}(u^2+u+a)=1$, the polynomial

$$X^2+\frac{1}{u^2+u+a}X+1\in\mathbb{F}_{2^k}[X]$$

is irreducible. Let $x\in\mathbb{F}_{2^{2k}}$ be a root of the above polynomial. The norm of x in $\mathbb{F}_{2^k}$ is $x^{2^k+1}=1$ and

$$x+x^{-1}=x+x^{2^k}=\frac{1}{u^2+u+a}.$$

Similarly, there exists $y\in\mathbb{F}_{2^{2k}}$ such that $y^{2^k+1}=1$ and

$$y+y^{-1}=\frac{1}{v^2+v+a}.$$

Let $x_1=x^d$ and $y_1=y^d$. Then $x_1^m=y_1^m=1$ and

$$\begin{aligned}1 + x_1 + x_1^{-1} + y_1 + y_1^{-1} &= 1 + x^d + x^{-d} + y^d + y^{-d} \\ &= 1 + D_d(x + x^{-1}) + D_d(y + y^{-1}) \\ &= 1 + D_d\Big(\frac{1}{u^2 + u + a}\Big) + D_d\Big(\frac{1}{v^2 + v + a}\Big) \\ &= 0.\end{aligned}$$

Hence m is a mad number. $\square$

We are now ready to give a proof of Theorem 4.2.

Proof of Theorem 4.2. From Lemma 4.4, it suffices to show that $H(U, V)$ has a root in $\mathbb{F}_{2^k}^2$. Write $q = 2^k$. Let $\overline{H}(U, V, W) \in \overline{\mathbb{F}}_2[U, V, W]$ be the homogenization of $H(U, V)$ and let

$$V_{\mathbb{P}^2(\mathbb{F}_q)}(\overline{H}) = \{(u : v : w) \in \mathbb{P}^2(\mathbb{F}_q) : \overline{H}(u, v, w) = 0\},$$
$$V_{\mathbb{F}_q^2}(H) = \{(u, v) \in \mathbb{F}_q^2 : H(u, v) = 0\}.$$

Since $\overline{H}$ is absolutely irreducible of degree $4d$,

$$\big||V_{\mathbb{P}^2(\mathbb{F}_q)}(\overline{H})| - q\big| \le (4d - 1)(4d - 2)q^{1/2} + \frac{1}{2} \cdot 4d(4d - 1)^2 + 1$$

by the Hasse-Weil bound and Bézout's theorem. (Note. The expression $\frac{1}{2} \cdot 4d(4d - 1)^2 + 1$ arises from the consideration of possible singular points on the curve $V_{\mathbb{P}^2(\mathbb{F}_q)}(\overline{H})$.) Therefore

$$\begin{aligned}|V_{\mathbb{P}^2(\mathbb{F}_q)}(\overline{H})| &\ge q - (4d - 1)(4d - 2)q^{1/2} - 2d(4d - 1)^2 - 1 \\ &= q^{1/2}(q^{1/2} - (4d - 1)(4d - 2)) - 2d(4d - 1)^2 - 1 \\ &\ge (4d)^2((4d)^2 - (4d - 1)(4d - 2)) - 2d(4d - 1)^2 - 1 \\ &= 10d(4d)^2 - (4d)^2 - 2d - 1 > 8d(4d)^2.\end{aligned}$$

Since $\overline{H}(U, V, 0) = U^{2d}V^{2d}$, $V_{\mathbb{P}^2(\mathbb{F}_q)}(\overline{H})$ contains only two points at ∞, namely, $(1 : 0 : 0)$ and $(0 : 1 : 0)$. Hence

$$|V_{\mathbb{F}_q^2}(H)| \ge |V_{\mathbb{P}^2(\mathbb{F}_q)}(\overline{H})| - 2 > 0. \qquad \square$$

Remark 4.5. The relation between mad numbers and Dickson polynomials has been observed in [1]. Indeed, the polynomial $g_n(X)$ defined in Section 5 of [1] is exactly $D_n(X)$. Theorem 5.1 in [1] states that m is mad if and only if $\gcd(D_m(X), D_m(X + 1)) \neq 1$. As pointed out by the referee, using this fact, one can determine if a given number is mad in polynomial time. Blokhuis and Brouwer have used Theorem 5.1 to generate a large amount of data.

5. Final remark

Let m, n be positive integers and let $q = 2^n$. The Dickson polynomial of the second kind of degree m with parameter 1 over $\mathbb{F}_q$ is defined to be

$$E_m(X) = \sum_{i=0}^{\lfloor m/2 \rfloor} \binom{m-i}{i} (-1)^i X^{m-2i}.$$

It is well known that

$$E_m(X + X^{-1}) = \frac{X^{m+1} - X^{-m-1}}{X - X^{-1}}.$$

(See [7] for more details.)

For $\alpha \in \mathbb{F}_q$, we can write $\alpha = \zeta + \zeta^{-1}$, where either $\zeta \in \mathbb{F}_q^*$ or $\zeta \in \mathbb{F}_{q^2}^*$ with $\zeta^{q+1} = 1$. If $\alpha \neq 0$, then $E_m(\alpha) = \frac{\zeta^{m+1} - \zeta^{-m-1}}{\zeta - \zeta^{-1}}$. So, $0 \neq \alpha$ is a root of $E_m(X)$ if and only if $\zeta^{m+1} = 1$. This implies that there is $\alpha \in \mathbb{F}_q^*$ satisfying $E_m(\alpha) = 0 = E_m(\alpha^{-1})$ if and only if there is $\alpha \in \mathbb{F}_q^*$ satisfying $D_{m+1}(\alpha) = 0 = D_{m+1}(\alpha^{-1})$.

Acknowledgments

We are grateful to Professor M. Freedman for the question that motivated this work. X. Cao would like to thank the Institute of Mathematics, Academia Sinica, for the financial support during his visit. A. Blokhuis and X. Hou would like to thank the Institute for Mathematical Sciences of the National University of Singapore for their hospitality and support and for facilitating their collaboration during their visit there. W.-S. Chou would express his gratitude to Dr. Y.-T. Lin of Institute of Mathematics, Academia Sinica, for helping the preparation of this paper. Finally, we are grateful to the anonymous referee for the valuable comments and suggestions which lead to the improvement of this paper.

References

[1] A. Blokhuis, A.E. Brouwer, Button madness, available at http://www.win.tue.nl/~aeb/preprints/madaart2c.pdf.
[2] W.-S. Chou, The factorization of Dickson polynomials over finite fields, Finite Fields Appl. 3 (1997) 84–96.
[3] W.-S. Chou, J. Gomez-Calderon, G.L. Mullen, Value sets of Dickson polynomials over finite fields, J. Number Theory 30 (1988) 334–344.
[4] M. Freedman, Private communication.
[5] G.H. Hardy, E.M. Wright, The Theory of Number, Oxford University Press, Oxford, UK, 1971.
[6] X. Hou, G.L. Mullen, J.A. Sellers, J.L. Yucas, Reversed Dickson polynomials over finite fields, Finite Fields Appl. 15 (2009) 748–773.
[7] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monogr. Surv. Pure Appl. Math., vol. 65, Longman Group UK Limited, 1993.
[8] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983.

[9] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1990) 43–53.
[10] The online encyclopedia of integer sequences, A001122, A093179, http://oeis.org/.
[11] D. Wiedemann, An iterated quadratic extension of GF(2), Fibonacci Quart. 26 (1988) 290–295.
[12] http://www.fermatsearch.org/factors/composite.php.