# Stability of $x^3 + x^2 + 1$ from the perspective of periodic sequences

Tong Lin[1] Qiang Wang[1]

**Abstract**

We have recently proved [10] the conjecture by Ahmadi and Monsef-Shokri [2] that $f(x) = x^3 + x^2 + 1$ is stable over $\mathbb{F}_2$. In this paper, we introduce a periodic sequence $(S_{k,n,i})_{i \geq -1}$ for each $k \in \mathbb{N}, n \in \mathbb{N}_0$ satisfying a non-linear recurrence relation, and establish connections between the stability of $f$ over $\mathbb{F}_{2^k}$ and properties of $(S_{k,n,i})_{i \geq -1}$ (namely, its recurrence relations, least period and distribution of zero terms). We also give equivalent characterizations of the roots of $(f_{k,n})_{n \geq 0}$ as well as closed-form formulas for $(S_{k,n,i})_{i \geq -1}$ in terms of the Fibonacci sequence.

## 1 Introduction and main results

We say a polynomial $t(x) \in \mathbb{K}[x]$, where $\mathbb{K}$ is a field, is stable over $\mathbb{K}$ if for each $n \in \mathbb{N}$, the $n$-th iterate $t^{(n)}(x) = t(t(\ldots t(t(x))))$ of $t$ is irreducible over $\mathbb{K}$. Problems concerning stability of polynomials over fields date back to the 1980s, when Odoni came up with one of the first examples [11, Proposition 4.1] and one of the first counter-examples [12, Corollary 1.6], respectively, of stable polynomials over a field. Stability of polynomials, especially those of low degrees, over various fields have been extensively studied ever since.

In 2012, Jones and Boston [8, Proposition 2.3] gave necessary and sufficient conditions for a quadratic polynomial to be stable over a finite field of odd characteristic in terms of the so-called adjusted critical orbits (using which Ostafe and Shparlinski [13, Corollary 2] estimated the complexity of testing stability of quadratic polynomials over a finite field of odd characteristic.) Then Ahmadi et al. [1, Theorem 4, Corollary 11] showed that *almost all* monic quadratic polynomials in $\mathbb{Z}[x]$ are stable over $\mathbb{Q}$ and that no quadratic polynomial is stable over a finite field of characteristic 2. In 2014, Goméz-Pérez and Nicolás, in collaboration with Ostafe and Sardonil [6, Theorem 5.5], estimated the number of stable polynomials of any degree $d \in \mathbb{N}$ over a finite field of odd characteristic.

When it comes to polynomials of degree greater than 2, determining whether they are stable over a field is more sophisticated than in the quadratic case. It is conjectured in [2, Conjecture 14] that $f(x) = x^3 + x^2 + 1$ is stable over $\mathbb{F}_2$, and a stability test based on *Capelli's Lemma* is proposed.

[1]School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa ON K1S 5B6, Canada.
The authors were supported by the Natural Sciences and Engineering Research Council of Canada (RGPIN-2017-06410).
*E-mail addresses*: tonglin4@cmail.carleton.ca (T. Lin), wang@math.carleton.ca (Q. Wang).

**Lemma 1.1** ([2, **Lemma 13**]). *Let $q > 1$ be a prime power, and let $F(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $d \in \mathbb{N}$. If $G(x) \in \mathbb{F}_q[x]$, then $F(G(x))$ is irreducible over $\mathbb{F}_q$ iff $G(x) - \alpha$ is irreducible over $\mathbb{F}_{q^d} \cong \mathbb{F}_q[x]/\langle F(x)\rangle$, where $\alpha$ is a root of $F(x)$ in $\mathbb{F}_{q^d}$.*

Let $k \in \mathbb{N}$. Using the above result, we construct a sequence $(\alpha_{k,n})_{n\geq 0}$ such that for each $n \in \mathbb{N}_0$, $\alpha_{k,n}$ is a root of $f^{(n)}$ in $\mathbb{F}_{2^{3^n k}}$ and that $f(\alpha_{k,n+1}) = \alpha_{k,n}$. Two new sequences $(\beta_{k,n})_{n\geq 0}$ and $(f_{k,n})_{n\geq 0}$ arise from $(\alpha_{k,n})_{n\geq 0}$. More precisely,

$$\beta_{k,n} = 1 + \alpha_{k,n} \in \mathbb{F}_{2^{3^n k}} \tag{1}$$

$$f_{k,n}(x) = x^3 + x + \beta_{k,n} \tag{2}$$

In [10], with the help of the above-mentioned sequences, we proved the following result having [2, Conjecture 14] as a special case.

**Theorem 1.2.** *Let $k \in \mathbb{N}$.*

*(1) If $3 \nmid k$, then $f_{k,n}$ is irreducible over $\mathbb{F}_{2^{3^n k}}$ for each $n \in \mathbb{N}_0$. In particular, $f(x) = x^3 + x^2 + 1$ is stable over $\mathbb{F}_{2^k}$.*

*(2) If $3 \mid k$, then $f_{k,n}$ splits completely into linear factors over $\mathbb{F}_{2^{3^n k}}$ for each $n \in \mathbb{N}_0$.*

We note that for each $k \in \mathbb{N}, n \in \mathbb{N}_0$, $xf_{k,n}(x) = x^4 + x^2 + \beta_{k,n}x$ is a linearized polynomial over $\mathbb{F}_{2^{3^n k}}$. From works in [7] and [14, Corollary 4] on inverses of linearized polynomials, we construct a sequence $(S_{k,n,i})_{i\geq -1}$, where

(1) $S_{k,n,-1} = 0$ and $S_{k,n,0} = 1$;

(2) $S_{k,n,i} = S_{k,n,i-1} + \beta_{k,n}^{2^{i-1}} S_{k,n,i-2}$.

**Remark 1.3.** *We note that every three consecutive terms in $(S_{k,n,i})_{i\geq -1}$ satisfy a different non-linear relation. However, $(S_{k,n,i})_{i\geq -1}$ can be defined by means of a single non-linear recurrence relation, namely, for each $i \in \mathbb{N}$,*

$$S_{k,n,i} = S_{k,n,i-1}^2 + \beta_{k,n}^2 S_{k,n,i-2}^4 \tag{3}$$

To view stability of $f$ over $\mathbb{F}_{2^k}$ (or equivalently, irreducibility of $(f_{k,n})_{n\geq 0}$) from the perspective of $(S_{k,n,i})_{i\geq -1}$, we present our main results.

**Theorem 1.4.** *Let $k \in \mathbb{N}$ be odd. For each $n \in \mathbb{N}_0$, $(S_{k,n,i})_{i\geq -1}$ is periodic, and if $t_{k,n}$ is its least period, then the following are equivalent.*

*(1) $f_{k,n}$ is irreducible over $\mathbb{F}_{2^{3^n k}}$;*

*(2) $xf_{k,n}(x)$ is a permutation polynomial over $\mathbb{F}_{2^{3^n k}}$;*

*(3) $S_{k,n,3^n k} + \beta_{k,n} S_{k,n,3^n k-2}^2 = 1$;*

*(4) $S_{k,n,3^n k-1} \neq 0$;*

*(5) $t_{k,n} = 3^{n+1}k$;*

*(6) $3 \nmid k$.*

*Moreover, $f$ is stable over $\mathbb{F}_{2^k}$ iff for each $n \in \mathbb{N}_0$, any of the above conditions holds.*

We remark that for general $k \in \mathbb{N}$, (1), (2), (3), (4), (6) are still equivalent and (5) implies all of them.

## 2 Properties of $(S_{k,n,i})_{i\geq -1}$

In order to structurally understand the solutions to the equation $x^{2^\ell+1}+x+a=0$ in $\mathbb{F}_{2^m}$, where $\ell<m$ are positive integers and $a\in\mathbb{F}_{2^m}^*$, a sequence of polynomials $(C_i(x))_{i=1}^{r+1}$, where $m=rd$ and $d=\gcd(\ell,m)$, defined over $\overline{\mathbb{F}_2}$ is introduced in [7, Equation (5)]. (We also note that a more general sequence is studied in [9].)

(1) $C_1(x)=C_2(x)=1$;

(2) $C_{i+2}(x)=C_{i+1}(x)+x^{2^{i\ell}}C_i(x)$ $(1\leq i\leq r-1)$.

Clearly, $(C_i(x))_{i=1}^{r+1}$ can be extended to an infinite sequence satisfying the above relations. Let $C_0(x)=0$. Let $k\in\mathbb{N}, n\in\mathbb{N}_0$. When $\ell=d=1$ and $m=r=3^nk$, induction yields that $S_{k,n,i}=C_{i+1}(\beta_{k,n})$. Moreover, the following results follow immediately from properties of $(C_i(x))_{i\geq 0}$.

**Proposition 2.1.** *For each $i\in\mathbb{N}$,*

*(1)* $S_{k,n,i}=S_{k,n,i-1}^2+\beta_{k,n}^2S_{k,n,i-2}^4$;

*(2)* $\beta_{k,n+1}^{2^i}=S_{k,n,i-1}\beta_{k,n+1}^2+\left(S_{k,n,i-2}^2\beta_{k,n}\right)\beta_{k,n+1}$;

*(3)* $S_{k,n,m}+\beta_{k,n}S_{k,n,m-2}^2\in\mathbb{F}_2$.

As a consequence of the above results, one can show that $(S_{k,n,i})_{i\geq -1}$ is periodic. For each $n\in\mathbb{N}_0$, let $\mathbb{F}_{2^{r_{k,n}}}$ be the smallest subfield of $\mathbb{F}_{2^{3^nk}}$ containing $\beta_{k,n}$.

**Proposition 2.2.** *For each $n\in\mathbb{N}_0$,*

*(1)* $r_{k,n+1}=r_{k,n}$ *or* $3r_{k,n}$;

*(2) if* $r_{k,n}<r_{k,n+1}$, *then* $(S_{k,n,i})_{i\geq -1}$ *is of least period* $r_{k,n+1}$;

*(3) if* $r_{k,n}=r_{k,n+1}$, *then* $S_{k,n,r_{k,n}}=1$ *or* $\beta_{k,n}^{-1}\beta_{k,n+1}$;

*(4) if* $r_{k,n}=r_{k,n+1}, S_{k,n,r_{k,n}}=1$, *then* $(S_{k,n,i})_{i\geq -1}$ *is of least period* $r_{k,n}$;

*(5) if* $r_{k,n}=r_{k,n+1}, S_{k,n,r_{k,n}}=\beta_{k,n}^{-1}\beta_{k,n+1}$, *then* $(S_{k,n,i})_{i\geq -1}$ *is of least period* $2r_{k,n}$.

While studying solutions to $x^3+x+a=0$, where $a\in\mathbb{F}_{2^m}^*$ for some $m\in\mathbb{N}$, Berlekamp et al. constructed the following polynomial sequence $(P_i(x))_{i\geq 1}$, which turns out to be also closely related to $(S_{k,n,i})_{i\geq -1}$.

**Theorem 2.3.** *[4, Theorem 4] Let $m\in\mathbb{N}$ and $a\in\mathbb{F}_{2^m}^*$. The polynomial $x^3+x+a$ splits completely into linear factors over $\mathbb{F}_{2^m}$ iff $P_m(a)=0$, where*

*(1)* $P_1(x)=P_2(x)=x$;

*(2)* $P_i(x)=P_{i-1}(x)+x^{2^{i-3}}P_{i-2}(x)$ *for each* $i\geq 3$.

In fact, if we add an initial term $P_0(x)=0$ to $(P_i(x))_{i\geq 1}$, then it is easy to see that the extended sequence $(P_i(x))_{i\geq 0}$ satisfies the above relations. By induction, the following holds.

**Proposition 2.4.** *For each $k\in\mathbb{N}, n,t\in\mathbb{N}_0$ and each $i\in\mathbb{N}_0\cup\{-1\}$,*

$$S_{k,n,i}^{2^{t-1}}=\beta_{k,n}^{-2^t}P_{i+1}\left(\beta_{k,n}^{2^t}\right) \tag{4}$$

Together, these propositions lead to Theorem 1.4.

# 3 Formulas for $(S_{k,n,i})_{i\geq -1}$

Let $k \in \mathbb{N}, n \in \mathbb{N}_0$. We give three closed-form formulas for $(S_{k,n,i})_{i\geq -1}$.

**Proposition 3.1.** *For each $i \in \mathbb{N}_0$, if $m = \left\lfloor \frac{i}{2} \right\rfloor$, then*

$$S_{k,n,i} = 1 + \sum_{j_1=1}^{i-1} \beta_{k,n}^{2^{j_1}} + \sum_{j_2=3}^{i-1} \sum_{j_1=1}^{j_2-2} \beta_{k,n}^{2^{j_1}+2^{j_2}} + \cdots + \sum_{j_m=2m-1}^{i-1} \cdots \sum_{j_1=1}^{j_2-2} \beta_{k,n}^{2^{j_1}+\cdots+2^{j_m}} \tag{5}$$

In fact, this result follows from a property of $(P_i(x))_{i\geq 1}$. Let $(B_i)_{i\geq 0}$ be such that $B_0 = 0$ and that the subsequence $(B_i)_{i\geq 1}$ is the ascending sequence of positive integers whose binary representations start with 1 and contain no consecutive 1's. Let $(F_i)_{i\geq 0}$ be the Fibonacci sequence. Then Eq. (5) is equivalent to the following.

**Proposition 3.2.** *For each $i \in \mathbb{N}_0 \cup \{-1\}$,*

$$S_{k,n,i} = \sum_{j=0}^{F_{i+1}-1} \beta_{k,n}^{2B_j} \tag{6}$$

A third formula of $(S_{k,n,i})_{i\geq -1}$ as a polynomial in $\beta_{k,n}^{-1}$ can also be derived to reduce computational complexity that comes with the usage of Eq. (6). Let $C_0 = 0$ and $(C_j)_{j\geq 1} = (1, 3, 5, 7, 11, \dots)$ be the ascending sequence of positive integers whose binary representations begin and end with 1 and contain no consecutive 0's.

**Proposition 3.3.** *If $T \in \mathbb{N}$ is a period of $(S_{k,n,i})_{i\geq -1}$, then*

$$S_{k,n,T-i} = \sum_{j=F_i}^{F_{i+1}-1} \beta_{k,n}^{-C_j 2^{T-(i-1)}} \qquad (0 \leq i \leq T) \tag{7}$$

# 4 Characterization of roots of $(f_{k,n})_{n\geq 0}$

Let $k \in \mathbb{N}$. In view of Theorem 1.2, studying stability of $f$ over $\mathbb{F}_{2^k}$ is equivalent to determining whether $f_{k,n}$ is irreducible over $\mathbb{F}_{2^{3^n k}}$ for each $n \in \mathbb{N}_0$. When $f_{k,n}$ is reducible over $\mathbb{F}_{2^{3^n k}}$, it is natural to ask what its roots are in $\mathbb{F}_{2^{3^n k}}$. Using the fact that $\beta_{k,n+1}^3 + \beta_{k,n+1} = \beta_{k,n}$ and that $\mathrm{Tr}_{3^n k}\left(\beta_{k,n}^{-1}\right) = \mathrm{Tr}_{3^n k}(1)$, one can show that if $f_{k,n}$ has a root in $\mathbb{F}_{2^{3^n k}}$, then it splits completely into linear factors over $\mathbb{F}_{2^{3^n k}}$. [10]

**Remark 4.1.** *According to [3, Equations 8, 9], we note that $f_{k,n}$ splits completely into linear factors over $\mathbb{F}_{2^{3^n k}}$ iff there exists some $v \in \mathbb{F}_{2^{3^n k}} \setminus \mathbb{F}_{2^2}$ such that*

$$\beta_{k,n} = \frac{v + v^{-1}}{(1 + v + v^{-1})^3} \tag{8}$$

*If Eq. (8) is satisfied, then the roots of $f_{k,n}$ in $\mathbb{F}_{2^{3^n k}}$ are*

$$x_0 = \frac{v + v^{-1}}{1 + v + v^{-1}}, \qquad x_1 = \frac{v}{1 + v + v^{-1}}, \qquad x_2 = \frac{v^{-1}}{1 + v + v^{-1}} \tag{9}$$

*Alternatively, if $x_0$ is a root of $f_{k,n}$ in $\mathbb{F}_{2^{3^n k}}$, then*

$$f_{k,n}(x) = (x + x_0)\left(x^2 + x_0 x + \left(x_0^2 + 1\right)\right) \tag{10}$$

*where the quadratic factor have two roots in $\mathbb{F}_{2^{3^n k}}$. Then by Vieta's formulas, the three roots of $f_{k,n}$ in $\mathbb{F}_{2^{3^n k}}$ are $x_0, u^2 x_0$ and $\left(1+u^2\right)x_0$. The two characterizations are equivalent, and the latter in fact follows from [5, Theorem 2.5], [9, Theorem 8].*

# References


[1] O. Ahmadi, F. Luca, A. Ostafe, I.E. Shparlinski, On stable quadratic polynomials, *Glasgow Mathematical Journal.* **54**(2): 359–369, 2012.

[2] O. Ahmadi, K. Monsef-Shokri, A note on the stability of trinomials over finite fields, *Finite fields and Their Applications.* **63**: 101649, 2020.

[3] E.R. Berlekamp, H. Rumsey, G. Solomon, Solutions of algebraic equations over fields of characteristic 2, *JPL Space Program Summary.* **IV**(37–39), 1966.

[4] E.R. Berlekamp, H. Rumsey, G. Solomon, On the solution of algebraic equations over finite fields, *Information and Control.* **10**(6): 553–564, 1967.

[5] A.W. Bluher, On $x^{q+1} + ax + b$, *Finite fields and Their Applications.* **10**(3): 285–305, 2004.

[6] D. Goméz-Pérez, A.P. Nicolás, A. Ostafe, D. Sardonil, Stable polynomials over finite fields, *Revista Matemática Iberoamericana.* **30**(2), 523–535, 2014.

[7] T. Helleseth, A. Kholosha, $x^{2^\ell+1}+x+a=0$ and related affine polynomials over GF $\left(2^k\right)$, *Cryptography and Communications.* **2**: 85–109, 2010.

[8] R. Jones, N. Boston, Settled polynomials over finite fields, *Proceedings of the American Mathematical Society.* **140**(6): 1849–1863, 2012.

[9] K.H. Kim, J. Choe, S. Mesnager, Solving $X^{q+1} + X + a$ over finite fields. *Finite Fields and Their Applications.* **70**: 101797, 2021.

[10] T. Lin, Q. Wang, On stability of $x^3 + x^2 + 1$, *https://arxiv.org/abs/2304.03992.*

[11] R.W.K. Odoni, On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \dots w_n$, *Journal of the London Mathematical Society. (Ser. 2)* **32**(1), 1–11, 1985.

[12] R.W.K. Odoni, The Galois theory of iterates and composites of polynomials, *Proceedings of the London Mathematical Society. (Ser. 3)* **51**(3) 385–414, 1985.

[13] A. Ostafe, I.E. Shparlinski, On the length of critical orbits of stable quadratic polynomials, *Proceedings of the American Mathematical Society.* **138**(8), 2653—2656, 2010.

[14] Y. Zheng, Q. Wang, W. Wei, On inverses of permutation polynomials of small degree over finite fields, *IEEE Transactions on Information Theory.* 66(2), 914–922, 2020.