# 1. Introduction

L'Enseignement Mathématique, t. 36 (1990), p. 53-65

# EXCEPTIONAL POLYNOMIALS AND THE REDUCIBILITY OF SUBSTITUTION POLYNOMIALS

by Stephen D. Cohen

## 1. Introduction

Let $\mathbf{F}_q$ be the finite field of prime power order $q = p^t$. Given a rational function $f = f_1/f_2$, where $f_1(x)$ and $f_2(x)$ are co-prime polynomials in $\mathbf{F}_q[x]$, define the substitution polynomials $\varphi_f$, $\varphi_f^*$ in two variables $x, y$ by $\varphi_f(x, y) = f_2(x)f_1(y) - f_1(x)f_2(y)$ and $\varphi_f^*(x, y) = \varphi_f(x, y)/(y-x)$. Usually, in fact, $f$ will simply be a polynomial (thus $f = f_1$) and always we assume, without loss, that $f$ is separable, i.e., $f(x) \notin \mathbf{F}_q(x^p)$. If $f = g(h)$ is functionally decomposable over $\mathbf{F}_q$, then $\varphi_f$ is divisible by $\varphi_h$, but reducibility of substitution polynomials not attributable to this phenomenon is apparently rare. Nevertheless, the concept of an exceptional polynomial (EP) calls for such reducibility, at least over $\bar{\mathbf{F}}_q$, the algebraic closure of $\mathbf{F}_q$. Specifically, a polynomial $f(x)$ in $\mathbf{F}_q[x]$ of degree $n > 1$ is called *exceptional* over $\mathbf{F}_q$ if none of the irreducible factors of $\varphi_f^*(x, y)$ over $\mathbf{F}_q$ is absolutely irreducible, i.e., remains irreducible over $\bar{\mathbf{F}}_q$. The importance of EPs derives from their connection with permutation polynomials (PPs) of $\mathbf{F}_q$. Briefly (see [8], Chap. 7, § 4), every EP over $\mathbf{F}_q$ is a PP and, conversely, for sufficiently large $q$ (as a function of $n$) every PP is an EP. Moreover, infinite classes of EPs are the most prominent in the list of known families of PPs compiled by Lidl and Mullen [7].

We distinguish below four families of polynomials over $\mathbf{F}_q$ whose substitution polynomials represent the chief examples of reducibility. These comprise the well-known classes of cyclic polynomials ($C_1$), Dickson polynomials ($C_2$) and linearised polynomials ($C_3$) together with a further (unnamed) class $C_4$ introduced in [1]. We denote their union $\bigcup_{i=1}^{4} C_i$ by $C$ and call the members of $C$ *$C$-polynomials*. $C$-polynomials are the source of all known

EPs with the understanding that those which are EPs can be combined by composition with each other and with linear polynomials to yield further EPs. Prompted by this last observation, we note that, because a composition $f = g(h)$ of polynomials over $\mathbf{F}_q$ is an EP if and only if both $g$ and $h$ are, [2], it suffices to classify EPs which are polynomially indecomposable. In group-theoretical terms, the restriction to indecomposable polynomials has the great advantage that $\mathrm{Gal}\left(f(y)-z/\mathbf{F}_q(z)\right)$, the Galois group of $f(y) - z$ over $\mathbf{F}_q(z)$, where $z$ is an indeterminate, is primitive as a permutation group on its roots, [2].

For $C$-polynomials, the reducibility of their substitution polynomials is of a fairly simple nature dominated by the existence (over $\bar{\mathbf{F}}_q$) of linear factors after the fashion we now indicate. As used in [1], a rational function (usually a polynomial) $f$ over $\mathbf{F}_q$ is called *factorable* if $\varphi_f(x, y)$ splits completely into factors in $\bar{\mathbf{F}}_q[x, y]$ which are linear (automatically in both $x$ and $y$). $C_1$-polynomials and $C_3$-polynomials are obviously factorable. $C_2$-polynomials and $C_4$-polynomials are not, since for these, $\varphi_f^*$ is the product over $\bar{\mathbf{F}}_q$ of irreducible polynomials of the same degree $d(>1)$, where $d = 2$ if $f$ is a Dickson polynomial. Nevertheless, they are "semi-factorable", a term to which we give the following definition. A rational function (here, always a polynomial) $f$ is called *semi-factorable* if there is a rational function $r(x)$ in $\mathbf{F}_q(x)$ such that the composition $f(r)$ is factorable over $\mathbf{F}_q$. As illustrated by the Dickson polynomials, rational functions $r$ may genuinely be required even when $f$ is a polynomial. Slanting the above facts another way, we observe that for an indecomposable $C$-polynomial $f$, $\mathrm{Gal}\left(f(y)-z/\mathbf{F}_q(z)\right)$ has abelian socle and so is an affine linear group (see [4]).

It was shown in [1] that, for any $f(x)$ in $\mathbf{F}_q[x]$, the product of the linear factors in $\varphi_f$ (its "factorable part") is wholly accounted for by the existence of polynomials $g(x)$, $h(x)$ in $\mathbf{F}_q(x)$ with $h$ factorable and $\varphi_h = \varphi_f$ such that $f = g(h)$; explicitly, $h = L^d$, where $L$ is a linearised (or linear) polynomial and $d \geqslant 1$. The main work of the present paper is an analysis (aided by group theory) of indecomposable polynomials whose substitution polynomials possess an irreducible quadratic factor over $\bar{\mathbf{F}}_q$. We shall conclude that these all lie in $C_2 \cup C_4$; thus, in particular, no new EPs arise in this way. The general treatment of substitution polynomials with factors of higher degree appears to be very difficult. Here, as we illustrate for polynomials with cubic factors, group theory seems to allow some exciting possibilities for reducibility but whether these can ever be realised for polynomials $f$ is another question (which is not treated here). Almost certainly, as we shall see, an indecomposable EP $f$ for which $\varphi_f$ has a cubic factor lies in $C_4$ but whether this extends is unclear. More generally, in connection with EPs two questions naturally arise.

(i) Are all indecomposable EPs over $\mathbf{F}_q$ semi-factorable?

(ii) Are all indecomposable semi-factorable EPs $C$-polynomials?

I would tentatively suggest that the answer to (ii) might be "yes" but hesitate to speculate on the answer to (i).

## 2. The semi-factorable families

The classes $C_1$, $C_2$ and $C_3$ are described briefly (see [8], for example). More detail is given for $C_4$.

$C_1$. *Cyclic polynomials.* These have the form $c_n(x) = x^n$, where $p \nmid n$. Obviously $c_n$ is factorable and is an EP (or PP) if and only if g.c.d. $(n, q-1) = 1$. Trivially, of course, $c_n$ is indecomposable over $\mathbf{F}_q$ if and only if $n$ is a prime $(\neq p)$.

$C_2$. *Dickson polynomials.* For any $n(>1)$ with $p \nmid n$ and any $a(\neq 0)$ in $\mathbf{F}_q$, a typical member $g_n(x, a)$ has the shape

$$g_n(x, a) = \sum_{i=0}^{[n/2]} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

As in [13], over $\bar{\mathbf{F}}_q$ we have

$$\varphi_{g_n}(x, y) = (y-x) \prod_{i=1}^{[n/2]} (y^2 - \alpha_i xy + x^2 + \beta_i^2 a), \tag{2.1}$$

where $\alpha_i = \zeta^i + \zeta^{-i}$, $\beta_i = \zeta^i - \zeta^{-i}$, $\zeta$ being a primitive $n$th root of unity in $\bar{\mathbf{F}}_q$. Since each of the quadratic factors in (2.1) is irreducible, $g_n$ is not factorable. Yet it is semi-factorable. Set $R(x) = g_n(r_a(x), a)$, where $r_a(x) = x + ax^{-1}$. Then, by equation (7.8) of [8],

$$R(x) = r_{a^n}(c_n(x)) = x^n + (a/x)^n$$

and hence

$$\varphi_R(x, y) = \prod_{i=0}^{n-1} (y - \zeta^i x)(xy - \zeta^i a).$$