IJMMS 27:4 (2001) 197–200
PII. S0161171201011309
http://ijmms.hindawi.com

CONSTRUCTING IRREDUCIBLE POLYNOMIALS WITH PRESCRIBED LEVEL CURVES OVER FINITE FIELDS

MIHAI CARAGIU

(Received 14 January 2001 and in revised form 28 March 2001)

ABSTRACT. We use Eisenstein's irreducibility criterion to prove that there exists an absolutely irreducible polynomial $P(X,Y) \in GF(q)[X,Y]$ with coefficients in the finite field $GF(q)$ with q elements, with prescribed level curves $X_c := \{(x,y) \in GF(q)^2 \mid P(x,y) = c\}$.

2000 Mathematics Subject Classification. 11T06.

1. Introduction. Let $GF(q)$ be the finite field with q elements. Assume that for any $c \in GF(q)$, a subset X_c (possibly empty) of the finite affine plane $GF(q)^2$ is given, such that $X_c \cap X_d \neq \emptyset$ for any $c \neq d$ and

$$GF(q)^2 = \bigcup_{c \in GF(q)} X_c. \tag{1.1}$$

In this paper, we use Eisenstein's irreducibility criterion to build absolutely irreducible polynomials

$$P(X,Y) \in GF(q)[X,Y] \tag{1.2}$$

such that for any $c \in GF(q)$ the level curve $\{(x,y) \in GF(q)^2 \mid P(x,y) = 0\}$ coincides with X_c. Note that $P(X,Y) \in GF(q)[X,Y]$ is called absolutely irreducible if it is irreducible over the algebraic closure of $GF(q)$.

If we define a function $f : GF(q)^2 \to GF(q)$ taking a constant value c on the set X_c for any $c \in GF(q)$, it is easy to see that this is equivalent to the fact that there exists an absolutely irreducible polynomial which interpolates the function f.

It is of course well known that there exists a polynomial that interpolates the function f (see [3, Section 7.5] for a general discussion on this topic). Thus, our result can be viewed as a stronger version of this basic fact, going back to Weber [4].

The basic facts about bivariate polynomial interpolation over finite fields that we will need are summarized in the following theorem.

THEOREM 1.1. *Any function $f : GF(q)^2 \to GF(q)$ can be interpolated by some polynomial in two variables. Moreover, there exists a unique polynomial $F(X,Y) \in GF(q)[X,Y]$ of degree less than q in both X and Y that interpolates the function f, that is, satisfying $F(a,b) = f(a,b)$ for any $(a,b) \in GF(q)^2$. Also, any two interpolating polynomials for f are congruent modulo the ideal of $GF(q)[X,Y]$ generated by $X^q - X$ and $Y^q - Y$.*

Our main result is the following theorem.

THEOREM 1.2. *Let $f : GF(q)^2 \to GF(q)$ be a function. Then there exists an absolutely irreducible polynomial $P(X,Y) \in GF(q)[X,Y]$ that interpolates the function f.*

2. Proof of the main result. Let $f : GF(q)^2 \to GF(q)$ be an arbitrary function. By Theorem 1.1, there exists a unique interpolating polynomial $H(X,Y) \in GF(q)[X,Y]$ for f, of degree at most $q-1$ in both X and Y. We order $H(X,Y)$ in terms of the powers of Y

$$H(X,Y) = c_0(X) + c_1(X)Y + \cdots + c_{q-1}(X)Y^{q-1}, \tag{2.1}$$

where $c_0(X), c_1(X), \ldots, c_{q-1}(X) \in GF(q)[X,Y]$ are of degree at most $q-1$.

Clearly, if we add $Y^q - Y$ to $H(X,Y)$, we still get an interpolating polynomial for f, say $K(X,Y)$, that is, monic in Y. Thus, it will be perfectly legitimate to start with an interpolating polynomial of the form

$$K(X,Y) = Y^q + d_{q-1}(X)Y^{q-1} + \cdots + d_1(X)Y + d_0(X), \tag{2.2}$$

where $d_0(X)$, $d_1(X), \ldots, d_{q-1}(X) \in GF(q)[X,Y]$ are of degree at most $q-1$.

It is well known (see [3, Corollary 2.11]) that there are irreducible polynomials of any degree over a finite field $GF(q)$. Fix such an irreducible polynomial $h(X) \in GF(q)[X]$ of degree 2. Clearly $h(X)$ has two roots in the algebraic closure of $GF(q)$, each of them generating the quadratic extension of $GF(q)$. Let α be a root of $h(X)$ in $\overline{GF(q)}$, the algebraic closure of $GF(q)$.

Our construction is based on replacing each polynomial coefficient $d_i(X)$ of (2.2) with a polynomial of the form

$$e_i(X) = d_i(X) + (X^q - X)u_i(X), \tag{2.3}$$

where $u_i(X) \in GF(q)[X]$, such that each $e_i(X)$ is divisible by $h(X)$ for $i = 0, \ldots, q-1$, while $e_0(X)$ is not divisible by $h(X)^2$. Clearly, the polynomial $F(X,Y)$ we get by performing these replacements

$$F(X,Y) = Y^q + e_{q-1}(X)Y^{q-1} + \cdots + e_1(X)Y + e_0(X) \tag{2.4}$$

will still be an interpolating polynomial for f, by Theorem 1.1. We will then see that $F(X,Y)$ follows to be absolutely irreducible.

We prove that for some choice of $u_i(X) \in GF(q)[X]$ in (2.3), $e_i(X)$ is divisible by $h(X)$, that is,

$$d_i(X) + (X^q - X)u_i(X) \equiv 0 \pmod{h(X)} \tag{2.5}$$

is solvable. Indeed, from the way we defined $h(X)$, $X^q - X$ is relatively prime to $h(X)$. Thus, (2.5) is a linear congruence modulo $h(X)$ in the Euclidean ring $GF(q)[X]$ in which the coefficient $X^q - X$ of the unknown $u_i(X)$ is relatively prime to the modulus $h(X)$. This being the case, a solution $u_i(X)$ of (2.5) exists, and is uniquely determined up to a multiple of $h(X)$. It follows that we can select a solution $u_i(X)$ of (2.5) which is

a polynomial of degree one. This will completely take care of the cases $i = 1,\dots,q-1$. For the special case $i = 0$ we are looking for a solution $u_0(X)$ of (2.5) satisfying the additional requirement

$$d_0(X) + (X^q - X)u_0(X) \not\equiv 0 \pmod{h(X)^2}. \tag{2.6}$$

This can be done as follows. If the solution $u_0(X)$ of the $i = 0$ case of (2.5) already satisfies (2.6) there is nothing to prove. Otherwise, if $u_0(X)$ satisfies

$$d_0(X) + (X^q - X)u_0(X) \equiv 0 \pmod{h(X)^2}, \tag{2.7}$$

just replace $u_0(X)$ with $u_0(X) + h(X)$. This last polynomial will satisfy both (2.5) and (2.6).

The last step in our proof will consist in showing that the polynomial $F(X,Y)$ constructed above is absolutely irreducible.

The key ingredient of this last step is *Eisenstein's irreducibility criterion* (see [2, Theorem 6.15]), to the effect that if $P(X) = \gamma_n X^n + \gamma_{n-1}X^{n-1} + \cdots + \gamma_1 X + \gamma_0$ is a polynomial with coefficients in some unique factorization domain $\mathbb{R}$, if we can find some irreducible element $p \in \mathbb{R}$ which divides $\gamma_0,\dots,\gamma_{n-1}$, does not divide γ_n, while p^2 does not divide γ_0, then $P(X)$ is an irreducible element of $R[X]$.

We view $F(X,Y)$ as a (monic) polynomial in Y with coefficients in the unique factorization domain $\overline{GF(q)}[X]$, that is, $F(X,Y) \in (\overline{GF(q)}[X])[Y]$.

Pick up the irreducible

$$p(X) := X - \alpha \in \overline{GF(q)}[X]. \tag{2.8}$$

Since α is a root of $h(X)$, by the way we constructed $F(X,Y)$ it follows that $p(X)$ divides the polynomial coefficients $e_0(X), e_1(X),\dots,e_{q-1}(X) \in GF(q)[X]$ and $p(X)^2$ does not divide the free coefficient $e_0(X)$. Also, the coefficient of the highest power of Y in (2.4) is 1. Thus, we can apply now Eisenstein's criterion to conclude that $F(X,Y)$ is an irreducible element of the polynomial ring $(\overline{GF(q)}[X])[Y] \cong \overline{GF(q)}[X,Y]$. In other words, the interpolating polynomial $F(X,Y)$ for f is absolutely irreducible. This concludes the proof of our main theorem. □

By our construction, the degrees of the polynomial coefficients $e_1(X),\dots,e_{q-1}(X)$ of $F(X,Y)$ are at most $q+1$, the degree of $e_0(X)$ is at most $q+2$, while $F(X,Y)$ is monic of degree q in Y.

Theorem 1.2 may be seen as a useful tool in the theory of curves over finite fields, since it allows a fairly elementary and efficient construction of equations of absolutely irreducible plane curves over $GF(q)$ with a given set $Z \subset GF(q)^2$ of $GF(q)$-rational points (we may, for example, apply our construction to the special case in which the level curves are $X_0 = Z$, $X_1 = GF(q)^2 \setminus Z$, and $X_c = \emptyset$ for any $c \in GF(q) \setminus \{0,1\}$). Finally, our interpolation result (with a construction based on a different method, though less direct) still holds true for the case of more than two variables (the proof of this will appear in [1]).

References

[1] M. Caragiu, *Multivariate interpolation by absolutely irreducible polynomials over finite fields*, to appear in Rev. Roumaine Math. Pures Appl.

[2] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, reprint of the 1974 original. MR 82a:00006. Zbl 442.00002.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. MR 97i:11115. Zbl 866.11069.

[4] H. Weber, *Lehrbuch der Algebra*, vol. 2, Vieweg & Sohn, Braunschweig, 1899.

Mihai Caragiu: The Institute of Mathematics at Bucharest, P.O. Box 1-764, RO-70700, Romania

Current address: Department of Mathematics, Ohio Northern University, Ada, OH 45810, USA

E-mail address: m-caragiu1@onu.edu