Pergamon

Chaos, Solitons & Fractals Vol. 9, No. 10, pp. 1769–1771, 1998
© 1998 Elsevier Science Ltd. All rights reserved
Printed in Great Britain
0960–0779/98 $19.00 + .00

PII: S0960-0779(96)00129-4

On a Remarkable Relation Between Future and Past Over Quadratic Galois Fields

METOD SANIGA*

Astronomical Institute, Slovak Academy of Sciences, SK-059 60 Tatranská Lomnica, The Slovak Republic

(Accepted 29 October 1996)

Abstract—It is demonstrated that the domain of the past of a pencil-generated temporal arrow over Galois fields of order q^2(GF(q^2)) incorporates the regions of *both* the past *and* the future of the arrow defined over its subfield GF(q). © 1998 Elsevier Science Ltd. All rights reserved

The starting point of this short contribution is the quadratic equation

$$ax^2 + bx + \vartheta = 0, a \neq 0 \neq b, \tag{1}$$

which, as is shown in detail in [1], gives us complete information about the structure of a temporal dimension generated by the pencil of conics[1],

$$Q^{\vartheta}_{\tilde{x}\tilde{x}}(q) \equiv \sum_{i,j=1}^{3} q_{ij}(\vartheta_{1,2})\check{x}_i\check{x}_j = \vartheta_1\check{x}_1\check{x}_2 + \vartheta_2\check{x}_3^2 = 0, \tag{2}$$

in a projective plane over an arbitrary Galois field GF(q), provided that the plane is affinized in the way that the equation of the 'line at infinity' reads

$$\check{x}_1 - a\check{x}_2 - b\check{x}_3 = 0, a \neq 0 \neq b \tag{3}$$

and where $\vartheta \equiv \vartheta_2/\vartheta_1$ and $x \equiv \check{x}_2/\check{x}_3$. In particular [1], if GF(q) is of an *odd* characteristic, then (Theorem 1):

- the domain of the past corresponds to Δ which are non-zero squares in GF(q), while
- the region of the future is represented by Δ non-squares in GF(q),

where $\Delta \equiv b^2 - 4a\vartheta$. On the other hand, when GF(q) has an *even* characteristic, then (Theorem 2):

- the domain of the past comprises the conics of pencil eqn (2), for which $D_q(\Theta) = 0$, whereas
- the region of the future is generated by those conics of eqn (2) whose $D_q(\Theta) = 1$, where $\Theta \equiv a\vartheta/b^2$ and

* Author for correspondence. E-mail: msaniga@auriga.ta3.sk.

[1] The symbols and notation adopted here are identical to those of [1].

$$D_q(\Theta) \equiv \Theta + \Theta^2 + \Theta^4 + \ldots + \Theta^{q/2}. \tag{4}$$

Let us deal first with the case when GF(q) has an even characteristic, i.e., when

$$q = 2^n, n = \text{some positive integer}. \tag{5}$$

Thus, for $\Theta \in \mathrm{GF}(q)$, eqn (4) acquires the form

$$D_q(\Theta) \equiv \Theta + \Theta^2 + \Theta^4 + \ldots + \Theta^{2^{n-1}}, \tag{6}$$

and for $\Theta \in \mathrm{GF}(q^2)$, we have

$$D_{q^2}(\Theta) \equiv \Theta + \Theta^2 + \Theta^4 + \ldots + \Theta^{2^{2n-1}}. \tag{7}$$

Our task is to rewrite eqn (7) in terms of eqn (6). To this end, we notice that

$$D_{q^2}(\Theta) \equiv (\Theta + \Theta^2 + \Theta^4 + \ldots + \Theta^{2^{n-1}}) + (\Theta^{2^n} + \Theta^{2^{n+1}} + \ldots + \Theta^{2^{2n-1}}) = D_q(\Theta) + (\Theta^{2^n} + (\Theta^2)^{2^n} + \ldots + (\Theta^{2^{n-1}})^{2^n}) \tag{8}$$

which, taking into account that in arithmetic modulo 2 [[1], eqn (11)]

$$(u + v + \ldots w)^2 = u^2 + v^2 + \ldots w^2, \tag{9}$$

can really be cast into the desired form,

$$D_{q^2}(\Theta) = D_q(\Theta) + D_q^{2^n}(\Theta). \tag{10}$$

At this point, it is only sufficient to recall that for elements w in a field of characteristic two ([1], Section 2)

$$w + w = 2w = 0, \tag{11}$$

in order to find that $D_{q^2}(\Theta) = 0$ for *both* $D_q(\Theta) = 0$ *and* $D_q(\Theta) = 1$. From Theorem 2, it then follows that GF(2^{2n})-*past contains both the* GF(2^n)-*past and* GF(2^n)-*future*. In the second part of this note, we will show that the same also holds for fields of odd characteristic, i.e., for

$$q = p^n, \tag{12}$$

p being a(ny) prime greater than 2.

To this end, we recall ([1], Section 2) that, for every Galois field GF(q), there exists a unique element η, called the primitive root, which has the property that any $x \in \mathrm{GF}(q)$ can be written as

$$x = \eta^k, k = \text{a positive integer}, \tag{13}$$

and which meets the constraint

$$\eta^{q-1} = 1. \tag{14}$$

Hence, denoting the primitive root of GF(q^2) as ρ, we have, for every $w \in \mathrm{GF}(q^2)$,

$$w = \varrho^l, l = \text{a positive integer} \tag{15}$$

and

$$\varrho^{q^2-1} = 1. \tag{16}$$

Combining eqn (14) and eqn (16) then yields

$$\eta = \varrho^{(q^2-1)/(q-1)} = \varrho^{q+1}, \tag{17}$$

from which it follows that

$$x = \eta^k = \varrho^{k(q+1)} \equiv \varrho^l = w. \tag{18}$$

Now, among the $q-1$ non-zero elements of GF(q), there are $(q-1)/2$ non-squares and the same number of squares, the former (latter) being the odd (even) powers of η [1]. Going back to eqn (18) and taking into account eqn (12), we see that because $q+1=p^n+1$ is even, l will be *even* irrespective of the character of k. Thus, both the non-squares and non-zero squares of GF(q) become squares in GF(q^2) which, in the light of Theorem 1, simply means that the GF(p^{2n})-*past*, $p>2$, also *incorporates both the* GF(p^n)-*past and* GF(p^n)-*future*.

Acknowledgement—This work was supported in part by the grant 2/506/93 of the Slovak Academy of Sciences.

REFERENCES

1. Saniga, M., Temporal dimension over Galois fields of characteristic two. *Chaos*, *Solitons & Fractals*, 1998, **9,** 1095–1104.