Note di Matematica ISSN 1123-2536, e-ISSN 1590-0932
Note Mat. **32** (2012) no. 2, 57–61. doi:10.1285/i15900932v32n2p57

Fractional Dimensional Semifield Planes

Linlin Chen
Department of Mathematics, University of Texas at Arlington
linlin.chen@mavs.uta.edu

Minerva Cordero
Department of Mathematics, University of Texas at Arlington
cordero@uta.edu

Received: 5.5.2011; accepted: 7.2.2012.

Abstract. We present a family of irreducible polynomials, where all the x-divisible monomials have trace zero, and use them to show that there are semifields of order 2^r, for any odd integer $r \in [5, 31]$ except 21 and 27, containing $GF(4)$. Hence these semifields are fractional dimensional.

Keywords: Knuth Semifields, fractional dimension

MSC 2000 classification: primary 17A35, secondary 51E15

Introduction

We know the dimension of the finite field $F = GF(q^n)$ over a subfield $K = GF(q)$ is specified by $log_{|K|}|F| = n$. One may more generally define the dimension of an arbitrary affine plane, relative to a subplane.

Definition 1.1 Let π be an affine plane of order n, with an affine subplane π_0 of order m. Then the dimension of π, relative to π_0 , is specified by $dim_{\pi_0}\pi = log_m n$.

Then π is said to have integral, fractional, or transcendental dimension, relative to π_0, according to $log_m n$ is an integer, a rational or a transcendental number.

If π is a translation plane of order p^n, and π_0 is an affine subplane, it follows that π_0 must have order p^m. Hence $dim_{\pi_0}\pi = m/n$, which is either an integer or a fractional number (not integer). In this article, we are interested in the latter case, i.e. when $dim_{\pi_0}\pi = m/n$ is a fractional number, not integer.

In this setting, Wene and Hentzel ([2]) found several sporadic semifields of order 2^j, for $j = 5, 7, 9, 11$, that admit a subplane of order 2^2. On the other hand, Jha and Johnson, pointed out a sufficient condition for the generalized Knuth Semifields admitting a subfield of order 2^2; see Theorem 1 ([1]).

In this article we find new parameters t for the affine Knuth semifield planes π of non-square odd order $GF(2^t)$, $t \geq 5$, to admit affine subplanes π_0 of order 2^2. This result follows from Lemma 1.

1 Preliminaries

Let $F = GF(2^t)$, t odd. The following defines a multiplication for a commutative semifield due to D.E. Knuth, called a "Knuth binary semifield". For any $x, y \in F$, define

$$x \circ y = xy + (xT(y) + yT(x))^2$$

where $T : GF(2^t) \longrightarrow GF(2)$ is the trace function.
Then a pre-semifield $(F, +, \circ)$ is obtained. Choose a nonzero element e in F and define a new multiplication $*$ by

$$x * y = (x' \circ e) * (e \circ y') = x' \circ y', \ \forall x, y \in F.$$

Then $(F, +, *)$ is a commutative semifield.

Jha and Johnson generalized Knuth's result, and obtained a new semifield as follows:

$$x \circ y = xbyc + (xbT(yc) + ycT(xb))^2, \ \forall x, y \in F$$

where b and c are nonzero constants in F. Define a multiplication $*$ as follows

$$(x \circ e) * (e \circ y) = x \circ y$$

where e is any nonzero element in F. Then $(F, +, *)$ is a semifield, which is not commutative.

In ([1]), they pointed out that if

$$T(ec) = T(b) = T(eb) = 0, \ T(c) = 1, \ \frac{e^2}{e+1} = 1 + \frac{b}{c}$$

then there exists a subfield isomorphic to $GF(4)$ in $(F, +, *)$.

The corresponding semifield plane is the commutative binary Knuth semifield plane, which has order 2^t, and would then admit a subsemifield plane of order 2^2.

When t is divisible by 5 or 7, say $t = 5k$ or $7k$, k odd, the results of the previous theorem show that there are subplanes of order 4 in the commutative binary Knuth semifield planes of order 2^t, c.f. Corollary 1 of ([1]).

2 New Examples

Lemma 1. *If $GF(2^t)$ is defined by an irreducible polynomial associated with $x^t + f(x) + 1$, where $f(x)$ is any x-divisible polynomial (the constant of $f(x)$ is 0) of degree$< t$, in which all even degree monomials have coefficients zero, then $T(x^i) = 0$, $0 < i < t$.*

Proof: For any x^i, $0 < i < t$,

$$T(x^i) = \sum_{j=0}^{t-1} (x^i)^{2^j} = x^i + (x^i)^2 + (x^i)^{2^2} + \cdots + (x^i)^{2^{t-1}}$$

Let $Gal(F)$={all the distinct automorphisms of $GF(2^t)$ over $GF(2)$} and σ be any element of $Gal(F)$. Then $\sigma(x) = x^{2^m}$, for any $m = 0, 1, \cdots, t-1$. Since t is odd, $\sigma(x)$ is x-divisible, and so is $T(x^i)$. Hence $T(x^i) = 0$, because the trace function is onto $GF(2)$. QED

Corollary 1. *If all the conditions of Lemma 1 are satisfied, then any monomial x^{2m} with even degree, except $2^k t$ for any integer k , has trace 0.*

Proof: Suppose $2m = qt + r$ for some integers q and r, $0 < r < t$. Then $x^{2m} = x^{qt}x^r$. So x^{2m} can be represented as an x-divisible polynomial with degree less than t; hence $T(x^{2m}) = 0$. QED

Lemma 2. *If an irreducible polynomia asl in Lemma 1 exists with $a_{2N-1} = 0$, i.e., $a_{t-2} = 0$, then $T(x^{t+2}) = 0$.*

Proof: Let $f(x) = \sum_{k=1}^{N} a_{2k-1}x^{2k-1}$. Then $x^t = 1 + \sum_{k=1}^{N} a_{2k-1}x^{2k-1}$, and

$$x^{t+2} = x^2x^t = x^2 + a_1x^3 + \cdots + a_{2t-3}x^{2N-1} + a_{2N-1}x^t$$

By Lemma 1, $T(x^i) = 0$, $0 < i < t$, so

$$T(x^{t+2}) = 0 + a_{2N-1}T(x^t) = 0 + 0 = 0.$$

QED

Theorem 1. *Suppose an irreducible polynomia as in Lemma 2 exists. Let*

$$e = 1 + x, b = x^{t+1} + x^{t-2}, c = x^t + x^{t-1}$$

Then the semifield $(F, +, *)$ admits a subfield isomorphic to $GF(4)$.

Proof: We just need to check that e, b and c satisfy the requirements in Theorem 1([1]):

Since $\frac{e^2}{1+e} = \frac{(1+x)^2}{x} = \frac{1+x^2}{x}$, and

$$\frac{b}{c} = \frac{x^{t+1} + x^{t-2}}{x^t + x^{t-1}} = \frac{x^{t-2}(x^3+1)}{x^{t-1}(x+1)} = \frac{x^2+x+1}{x}$$

we have $\dfrac{e^2}{1+e} = 1 + \frac{b}{c}$. Also

$$T(b) = T(x^{t+1}) + T(x^{t-2}) = 0 + 0 = 0,$$
$$T(c) = T(x^t) + T(x^{t-1}) = 1 + 0 = 1,$$
$$T(ec) = T((1+x)(x^t + x^{t-2})) = T(x^{t+1}) + T(x^{t-1}) = 0.$$

By Lemma 2,

$$T(eb) = T(x^{t+1}) + T(x^{t-2}) + T(x^{t+2}) + T(x^{t-1}) = 0.$$

QED

This theorem works for some particular orders of generalized Knuth binary semifields. The following corollary lists $f(x)$ in the irreducible polynomials of $x^t + f(x) + 1$ associated with $GF(2^t)$, t odd.

Corollary 2. *If $f(x)$ as in Lemma 2 exists, then the semifield $(F, +, *)$ with e, b, and c as defined above is a fractional semifield of order 2^{tk} for each odd $k \geq 1$. Examples of such $f(x)$ include:*

$$
\begin{array}{ll}
t = 7, 9, 15, & f(x) = x + 1 \\
t = 11, & f(x) = x^5 + x^3 + x + 1 \\
t = 13, & f(x) = x^7 + x^3 + x + 1 \\
t = 17, 25, 31, & f(x) = x^3 + 1 \\
t = 19, & f(x) = x^9 + x^7 + x + 1 \\
t = 23, & f(x) = x^5 + 1 \\
t = 29, & f(x) = x^{27} + x + 1
\end{array}
$$

3 Irreducible Polynomials with Even Degree Monomials

The condition of non-even monomials imposed on the polynomial $f(x)$ on Lemma 1 is not necessary for the existence of fractional dimensional planes of order 2^t. For example, in ([1]), Jha and Johnson chose $x^7 + x^4 + x^3 + x^2 + 1$ as the irreducible polynomial over $GF(2)$ associated with $GF(2^{7k})$, k odd, and $e = 1 + x^7$, $b = x^7$, and $c = x^3$ satisfy all the requirements of Theorem 1 on [1]. For $GF(2^{13k})$, k odd, we can choose the irreducible polynomial $x^{13}+x^4+x^3+x+1$ over $GF(2)$, and $e = 1 + x^{11}$, $b = 1 + x + x^7 + x^9$, $c = x^7 + x^9$.
The corresponding generalized Knuth semifield of order 2^{13k}, k odd, also admits a subfield of order 4.

Acknowledgements. The authors would like to express their sincere gratitude to the referee for the valuable recommendations which greatly improved the presentation and content of this paper.

References

[1] V. Jha, N.L. Johnson: *The dimension of a subplane of a translation plane*, Bull. Belg. Math. Soc. Simon Stevin **17**, 2010, n. 3, 463–477.

[2] g. Wene, I. Hentzel: *Albert's construction for semifields of even order*, Comm. in Algebra **38**, 2010, no.5 , 1790-1795.