Note di Matematica **27,** n. 1, 2007, 53–59.

Counting the generalized twisted fields

William Purpura
Department of Mathematics, University of Texas at Arlington
Arlington, TX, 76019, USA
bpurpura@uta.edu

Received: 3/12/2005; accepted: 15/3/2006.

Abstract. In this paper we exploit a theorem of Biliotti, Jha, and Johnson exhibiting a procedure to count the number of non-isotopic generalized twisted fields of orders p^n where $p \geq 3$ which is denoted by $g(p^n)$. We show that $g(p^n)$ is a polynomial in p that is sharply bounded below by $\binom{n-2}{2}(p-2)$ and bounded above by a polynomial of degree $\lfloor \frac{n}{2} \rfloor$.

Keywords: semifield, generalized twisted field, projective plane, finite geometry

MSC 2000 classification: primary 12K10, secondary 51E15

Introduction

A particularly interesting class of semifields are Albert's generalized twisted fields defined in [1]. They exist for all prime power orders $p^n > \max(p^2, 8)$ except for 2^q where q is prime. We determine the number of non-isotopic generalized twisted fields of order p^n where p is odd. Our result enables us, among other things, to obtain a sharp lower bound for the number of non-isomorphic generalized twisted field planes of odd characteristic:

1 Theorem. *The number of non-isotopic generalized twisted fields of order p^n is at least $\binom{n-2}{2}(p-2)$, and the bound is sharp if and only if n is prime or $n = 4$.*

Our argument is based on a theorem of Biliotti, Jha, and Johnson [2] where a necessary and sufficient condition is given for two generalized twisted fields to be isotopic. Thus, our goal is to count the number of equivalence classes associated with the isotopism classes among the generalized twisted fields. First we list some number theory that will be used throughout the paper.

2 Theorem. [7, Proposition 3.3.1] *Let $a, b \in \mathbb{Z}$, let $d = (a, m)$, and let $m' = m/d$. The equation $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$. If the equation is solvable, then there are exactly d solutions. Furthermore, if x_0 is a solution then the other solutions are $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$.*

3 Theorem. [3, Result 25.5.1] *Let p be a prime number. Then*

$$(p^{i_1} - 1, p^{i_2} - 1, \ldots, p^{i_t} - 1) = p^{(i_1, i_2, \ldots, i_t)} - 1.$$

4 Corollary. *The subgroup of* $\mathbb{Z}_{p^n-1}$ *generated by* $p^{i_1}-1, p^{i_2}-1, \ldots, p^{i_t}-1$ *is the subgroup generated by* $p^{(i_1,i_2,\ldots,i_t,n)}-1$.

5 Corollary. $i \mid j$ *if and only if* $p^i - 1 \mid p^j - 1$.

1 Generalized Twisted Fields

Throughout this paper F will be a field of odd characteristic with a primitive element γ such that $|F| = p^n > p^2$. Let $F = \mathrm{GF}(p^n)$. Let $\gamma^s \mapsto \gamma^{sp^i}$ and $\gamma^s \mapsto \gamma^{sp^j}$ be distinct non-identity automorphisms of F where $0 < i, j < n$. Let $\gamma^r \in F - \{0\}$ such that

$$\gamma^r \neq \gamma^{a(p^i-1)}\gamma^{b(p^j-1)} \text{ for all } a, b \in \mathbb{Z} \tag{1}$$

Define a new multiplication $\circ$ on F by

$$\gamma^a \circ \gamma^b = \gamma^{a+b} - \gamma^{r+ap^i+bp^j} \tag{2}$$

We now pass this to a semifield by defining $(\gamma^a \circ 1) \star (1 \circ \gamma^b) = \gamma^a \circ \gamma^b$ [5]. The semifield $(F, +, \star)$ which we denote by $A(F, i, j, \gamma^r)$ is called a *generalized twisted field*. When we say γ^r makes $A(F, i, j, \gamma^r)$ into a generalized twisted field, we mean that γ^r satisfies (1).

We now give a necessary and sufficient condition that γ^r must satisfy in order to make $A(F, i, j, \gamma^r)$ into a generalized twisted field.

6 Lemma. $A(F, i, j, \gamma^r)$ *is a generalized twisted field if and only if* $r \not\equiv 0 \pmod{p^{(i,j,n)} - 1}$.

Proof. The condition (1) is equivalent to $r \not\equiv a(p^i-1)+b(p^j-1) \pmod{p^n-1}$ for all $a, b \in \mathbb{Z}$. Now apply corollary 4. $\boxed{QED}$

7 Corollary. $A(F, i, j, \gamma)$ *is always a generalized twisted field.*

2 Counting the Generalized Twisted Fields

The counting results that are obtained stem from the following result which is equivalent to one of Biliotti, Jha, and Johnson [2, Theorem 6.1 (2)]:

8 Theorem (Comparison Theorem)**.** *Let* $F = \mathrm{GF}(p^n)$. *Two generalized twisted fields* $A(F, i, j, \gamma^r)$ *and* $A(F, i', j', \gamma^{r'})$ *are isotopic if and only if one of the following conditions is met:*

(i) $i' = i$, $j' = j$, *and* $r'p^k \equiv r + a(p^i-1) + b(p^j-1) \pmod{p^n-1}$ *for some* $0 \leq a, b < p^n - 1$, *and* $0 \leq k < n$.

(ii) $i' = n - i$, $j' = n - j$, *and* $r'p^k \equiv -r + a(p^i - 1) + b(p^j - 1) \pmod{p^n - 1}$ *for some* $0 \leq a, b < p^n - 1$, *and* $0 \leq k < n$.

9 Lemma. $A(F, i, j, \gamma^{r'}) \simeq A(F, i, j, \gamma^r)$ *if and only if* $r'p^k \equiv r \pmod{p^{(i,j,n)} - 1}$ *for some* $0 \leq k < (i, j, n)$.

Proof. The condition $r'p^k \equiv r + a(p^i - 1) + b(p^j - 1) \pmod{p^n - 1}$ is equivalent to $r'p^k - r \equiv a(p^i - 1) + b(p^j - 1) \pmod{p^n - 1}$. By corollary 4 this holds if and only if $r'p^k \equiv r \pmod{p^{(i,j,n)} - 1}$. $\boxed{QED}$

10 Corollary. $A(F, i, j, \gamma^r)$ *is isotopic to* $A(F, n - i, n - j, \gamma^{r'})$ *if and only if* $r'p^k \equiv -r \pmod{p^{(i,j,n)} - 1}$ *for some* $0 \leq k < (i, j, n)$.

Proof. Same as above since $(n - i, n - j, n) = (i, j, n)$. $\boxed{QED}$

11 Corollary. *The following statements hold:*

(i) *If* $r' \equiv r \pmod{p^{(i,j,n)} - 1}$ *then* $A(F, i, j, \gamma^{r'}) \simeq A(F, i, j, \gamma^r)$.

(ii) *For fixed* i, j *the set* $\{ A(F, i, j, \gamma), A(F, i, j, \gamma^2), \ldots, A(F, i, j, \gamma^{p^{(i,j,n)} - 2}) \}$ *contains at least one representative of the isotopy class of* $A(F, i, j, \gamma^r)$ *for any* $r \neq 0 \pmod{p^{(i,j,n)} - 1}$.

Proof. (i) follows immediately from lemma 9, taking $k = 0$, and (ii) follows from (i). $\boxed{QED}$

As a result of this corollary we will assume henceforth that $0 \leq r < p^{(i,j,n)} - 1$, and all exponents of γ will be taken modulo $p^{(i,j,n)} - 1$.

12 Lemma. *If* $A(F, n - i, n - j, \gamma^{r'})$ *is a generalized twisted then so is* $A(F, i, j, \gamma^{-r'})$. *Furthermore*

$$A\left(F, n - i, n - j, \gamma^{r'}\right) \simeq A\left(F, i, j, \gamma^{-r'}\right) \tag{3}$$

Proof. This follows immediately from lemma 6 and the comparison theorem. $\boxed{QED}$

13 Definition. Let $g(i, j, p^n)$ denote the number of non-isotopic generalized twisted field of order p^n of the type $A(F, i, j, \gamma^r)$ with i, j fixed. Also, let $g(p^n)$ denote the number of non-isotopic generalized twisted fields of order p^n.

14 Lemma. $g(p^n) = \sum_{1 \leq i < j < n} g(i, j, p^n)$.

Proof. The comparison theorem and lemma 12 immediately yield this. $\boxed{QED}$

We now wish to determine $g(i, j, p^n)$. By corollary 11 (ii), $g(i, j, p^n) \leq |\mathfrak{C}| = p^{(i,j,n)} - 2$ where $\mathfrak{C} = \{ A(F, i, j, \gamma), \ldots, A(F, i, j, \gamma^{p^{(i,j,n)} - 2}) \}$. Also by corollary 11 (ii) we may assume that $1 \leq r \leq p^{(i,j,n)} - 2$. By lemma 9, $A(F, i, j, \gamma^{r'}) \simeq A(F, i, j, \gamma^r)$ if and only if $r'p^k \equiv r \pmod{p^{(i,j,n)} - 1}$ for some $0 \leq k < (i, j, n)$.

So we need to determine if $\mathfrak{C}$ contains *exactly* one representative from every isotopy class.

To determine which generalized twisted fields are isotopic to $A(F,i,j,\gamma^r)$ we need to compute $\{rp^k \pmod{p^{(i,j,n)}-1} : 0 \leq k < (i,j,n)\}$. Clearly $\{\, s : A(F,i,j,\gamma^r) \simeq A(F,i,j,\gamma^s)\,\} = \{\, s : rp^k \equiv s \pmod{p^{(i,j,n)}-1} \text{ for some } k\,\} = \{\, rp^k : 0 \leq k < (i,j,n)\,\}$. From this we gather $A(F,i,j,\gamma^{rp^k \pmod{p^{(i,j,n)}-1}}) \simeq A(F,i,j,\gamma^r)$.

In doing this computation, if for a particular k, $rp^k \equiv r \pmod{p^{(i,j,n)}-1}$, then nothing new happens, since this isotopy is already captured by corollary 11. However, if $rp^k \neq r \pmod{p^{(i,j,n)}-1}$ for some k then we get that $A(F,i,j,\gamma^{rp^k \pmod{p^{(i,j,n)}-1}}) \simeq A(F,i,j,\gamma^r)$, so one of these elements needs to be removed from $\mathfrak{C}$. Thus the problem now is determining the solutions in r to $rp^k \equiv r \pmod{p^{(i,j,n)}-1}$.

15 Lemma. *The solutions for r of $rp^k \equiv r \pmod{p^{(i,j,n)}-1}$ are exactly those of $rp^{(i,j,k,n)} \equiv r \pmod{p^{(i,j,n)}-1}$.*

Proof. By theorem 2, both $r(p^k-1) \equiv 0 \pmod{p^{(i,j,n)}-1}$ and $r(p^{(i,j,k,n)}-1) \equiv 0 \pmod{p^{(i,j,n)}-1}$ have $p^{(i,j,k,n)}-1$ solutions. Since 0 is a solution to both of these congruences, they must be the same. $\boxed{QED}$

If we let k run between 1 and (i,j,n) we have that (i,j,k,n) runs precisely through all the divisors of (i,j,n). Thus by lemma 15 it suffices to consider congruences of the form $rp^k \equiv r \pmod{p^{(i,j,n)}-1}$ where k is a divisor of (i,j,n).

16 Lemma. *Let d_1 and d_2 be divisors of (i,j,n). Then $d_1|d_2$ if and only if every solution of $rp^{d_1} \equiv r \pmod{p^{(i,j,n)}-1}$ is a solution of $rp^{d_2} \equiv r \pmod{p^{(i,j,n)}-1}$.*

Proof. If $d_1|d_2$ then the result is trivial so suppose the converse. Thus, every solution of $rp^{d_1} \equiv r \pmod{p^{(i,j,n)}-1}$ is a solution to $rp^{d_2} \equiv r \pmod{p^{(i,j,n)}-1}$. These congruences have $p^{d_1}-1$ and $p^{d_2}-1$ solutions respectively. Then the solutions to $rp^{d_1} \equiv r \pmod{p^{(i,j,n)}-1}$ form a subgroup of the solutions to $rp^{d_2} \equiv r \pmod{p^{(i,j,n)}-1}$. By Lagrange's theorem we have $p^{d_1}-1|p^{d_2}-1$. By corollary 5, $d_1|d_2$ as desired. $\boxed{QED}$

17 Definition. Let r be given. We define $k_0(r)$ to be the minimal k such that $rp^k \equiv r \pmod{p^{(i,j,n)}-1}$.

18 Lemma. *The isotopy class of $A(F,i,j,\gamma^r)$ is*

$$\overline{A(F,i,j,\gamma^r)} = \left\{ A\left(F,i,j,\gamma^r\right), A\left(F,i,j,\gamma^{rp}\right), \ldots, A\left(F,i,j,\gamma^{rp^{k_0(r)-1}}\right) \right\},$$

where the exponents of γ are taken modulo $p^{(i,j,n)}-1$. Furthermore, every element $A(F,i,j,\gamma^{rp^k}) \in \overline{A(F,i,j,\gamma^r)}$ satisfies $k_0(rp^k) = k_0(r)$.

Proof. Let Ω denote the isotopy class of $A(F, i, j, \gamma^r)$. Certainly

$$\overline{A\,(F, i, j, \gamma^r)} \subseteq \Omega$$

by lemma 9.

Let $A(F, i, j, \gamma^s) \in \Omega$. By lemma 9 it follows that $rp^k \equiv s \pmod{p^{(i,j,n)} - 1}$ but $A(F, i, j, \gamma^s) \simeq A(F, i, j, \gamma^{s \pmod{p^{(i,j,n)}-1}}) \in \overline{A(F, i, j, \gamma^r)}$. This shows that $\Omega \subseteq \overline{A(F, i, j, \gamma^r)}$.

We show that $k_0(rp^k) = k_0(r)$ for all $A(F, i, j, \gamma^{rp^k}) \in \overline{A(F, i, j, \gamma^r)}$. Since $rp^{k_0(r)} \equiv r \pmod{p^{(i,j,n)} - 1}$ we have that $(rp^k)p^{k_0(r)} \equiv rp^k \pmod{p^{(i,j,n)} - 1}$. This shows that $k_0(rp^k) \leq k_0(r)$. If $k_0(rp^k) < k_0(r)$ for some rp^k then we would have $(rp^k)p^{k_0(rp^k)} \equiv rp^k \pmod{p^{(i,j,n)} - 1}$. This implies that $rp^{k_0(rp^k)} \equiv r \pmod{p^{(i,j,n)} - 1}$ which contradicts the definition of $k_0(r)$. QED

19 Corollary. *The size of the isotopy class of $A(F, i, j, \gamma^r)$ is $k_0(r)$.*

To find $g(i, j, p^n)$ we need to divide the r's into different classes; we find how many r's minimally satisfy a given congruence $rp^k \equiv r \pmod{p^{(i,j,n)} - 1}$ for k a divisor of (i, j, n). We mean minimally in the sense that $k_0(r) = k$. There are exactly $p^k - 1$ solutions to $rp^k \equiv r \pmod{p^{(i,j,n)} - 1}$ for a fixed k, but only some of these r's will satisfy $k_0(r) = k$. So to find the number of r's that satisfy $k_0(r) = k$ we must first find the r's such that $k_0(r) < k$. We specify recursively a function $\Psi_{ij} : \mathbb{N} \to \mathbb{N}$ which corresponds to the number of r's such that $k_0(r) = d$.

$$\Psi_{ij}(d) = p^d - 1 - \sum_{k|d, k \neq d} \Psi_{ij}(k) \tag{4}$$

We note that $\Psi_{ij}(1) = p - 1$ so Ψ_{ij} is clearly defined for all natural numbers.

20 Theorem. $g(i, j, p^n) = \left(\sum_{d|(i,j,n)} \frac{\Psi_{ij}(d)}{d}\right) - 1.$

Proof. For a given divisor d of (i, j, n), there will be $\Psi_{ij}(d)$ r's such that $k_0(r) = d$. Each of these will have an isotopy class of size d by corollary 19. Thus we get precisely $\frac{\Psi_{ij}(d)}{d}$ isotopy classes from the divisor d. Since $r \neq 0$ by lemma 6 we get the formula

$$g(i, j, p^n) = \left(\sum_{d|(i,j,n)} \frac{\Psi_{ij}(d)}{d} \right) - 1 \tag{5}$$

as desired. QED

21 Corollary. $g(p^n) = \sum_{1 \leq i < j < n} \left(\left(\sum_{d|(i,j,n)} \frac{\Psi_{ij}(d)}{d} \right) - 1 \right).$

Proof. Just use the above theorem along with lemma 14. QED

We now give some solutions for $g(i,j,p^n)$ where (i,j,n) is relatively simple:

22 Theorem. *Let $(i,j,n) = p_1^t$, a prime power. Then*

$$g(i,j,p^n) = p - 2 + \sum_{s=1}^{t} \frac{\left(p^{p_1^s} - 1\right) - \left(p^{p_1^{s-1}} - 1\right)}{p_1^s} \tag{6}$$

23 Corollary. *Let $(i,j,n) = p_1$ prime. Then*

$$g(i,j,p^n) = (p-2) + \frac{p^{p_1} - 1 - (p-1)}{p_1} \tag{7}$$

24 Theorem. *If $(i,j,n) = 1$ then $g(i,j,p^n) = p-2$. Thus if $p = 3$ then the unique generalized twisted field is $A(F,i,j,\gamma)$.*

25 Corollary. *Let n be prime or $n = 4$. Then $g(p^n) = \binom{n-2}{2}(p-2)$.*

Proof. Since n is prime or $n = 4$, then $(i,j,n) = 1$ for all i,j pairs. Now apply the theorem along with lemma 14. $\boxed{QED}$

26 Corollary. *$g(p^n)$ is bounded below by $\binom{n-2}{2}(p-2)$. Furthermore, this bound is sharp and is attained if and only if n is prime or $n = 4$.*

Proof. By corollary 21, we have $g(p^n)$ is completely determined by the prime factorizations of the (i,j,n)'s where $1 \le i < j < n$. By theorem 20, $g(i,j,p^n) \ge p-2$ with equality occurring if and only if $(i,j,n) = 1$. Therefore, $g(p^n) \ge \binom{n-2}{2}(p-2)$ and equality occurs if and only if (i,j,n) is 1 for all i,j such that $1 \le i < j < n$. We show this happens precisely when n is prime or $n = 4$.

Clearly, if n is prime or 4 then $(i,j,n) = 1$ for all $1 \le i < j < n$. Conversely, suppose n is not prime and $n \ne 4$. Then it follows that $n > 4$. Let f be the smallest prime divisor of n. We have that $n > 2f$ so that $(f, 2f, n) = f \ne 1$. Now the result follows. $\boxed{QED}$

27 Theorem. *$g(p^n)$ is a polynomial in p of degree $\mu(n)$ where $\mu(n)$ is defined as the largest divisor of n which is strictly less than $n/2$.*

Proof. Observe that $g(i,j,p^n)$ is a polynomial of degree (i,j,n). We thus have $g(p^n)$ is a polynomial of degree d where $d = \max_{1 \le i < j < n}(i,j,n)$. It is clear that $\mu(n) = d$. $\boxed{QED}$

28 Corollary. *If $\mu(n_1) > \mu(n_2)$ then $g(p^{n_1}) > g(p^{n_2})$ for $p >> 0$.*

Proof. This follows by the above theorem and elementary calculus. $\boxed{QED}$

This Corollary is counter-intuitive. It shows that $g(p^n)$ is not as dependent on the magnitude of n as on the prime factorization of n. For example, we gather that $g(p^6) > g(p^q)$ for $p >> 0$ for any prime q.

29 Corollary. *$g(p^n)$ is bounded above by a polynomial of degree $\lfloor \frac{n}{2} \rfloor$.*

Proof. Since $g(p^n)$ is a polynomial of degree $\mu(n)$ and clearly $\lfloor \frac{n}{2} \rfloor > \mu(n)$ we get the required polynomial is $g(p^n)p^{\lfloor \frac{n}{2} \rfloor - \mu(n)}$. $\boxed{QED}$

References

[1] A. A. Albert: *Generalized Twisted Fields*, Pacific J. Math, **11** (1961), 1–8.

[2] M. Biliotti, V. Jha, N. L. Johnson, *The collineation groups of generalized twisted field planes*, Geom. Dedicata, **76** (1999), 97–126.

[3] M. Biliotti, V. Jha, N. L. Johnson: Foundations of Translation Planes, Marcel Dekker, 2001.

[4] M. Cordero, G. Wene, *A survey of finite semifields*, Discrete Mathematics, **208/209** (1999), 125–137.

[5] P. Dembowski: Finite Geometries, Springer, 1968.

[6] D. R. Hughes, F. C. Piper, Projective Planes, Springer-Verlag, 1973.

[7] K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory, Springer-Verlag, 1972.

[8] D. Knuth, *Finite semifields and projective planes*, J. Algebra, **2** (1965), 182–217.