J. Aust. Math. Soc. **82** (2007), 297–313

EXTENDING ABELIAN GROUPS TO RINGS

LYNN M. BATTEN, ROBERT S. COULTER✉ and MARIE HENDERSON

(Received 21 April 2005; revised 10 November 2005)

Communicated by E. A. O'Brien

Abstract

For any abelian group G and any function $f : G \to G$ we define a commutative binary operation or 'multiplication' on G in terms of f. We give necessary and sufficient conditions on f for G to extend to a commutative ring with the new multiplication. In the case where G is an elementary abelian p-group of odd order, we classify those functions which extend G to a ring and show, under an equivalence relation we call weak isomorphism, that there are precisely six distinct classes of rings constructed using this method with additive group the elementary abelian p-group of odd order p^2.

2000 *Mathematics subject classification*: primary 11T30; secondary 13A99.

1. Introduction

The classification of finite simple groups was primarily motivated by the fact that simple groups are the essential building blocks of finite groups. For finite ring theory, the rings of prime power order assume the role of simple groups as the prime objects. Recently, the problem of classifying finite associative rings has received considerable attention, see [5, 6, 19] for example. Meanwhile, work on non-associative rings has tended to concentrate more on construction methods, though there have been some results on the classification problem, such as [11]. In their broadest sense, rings can be viewed as additive groups with an additional bivariate mapping satisfying specific properties used for multiplication. Here we provide a method for constructing non-associative rings based on this viewpoint and then consider the classification problem for the resulting rings, concentrating specifically on the elementary abelian case. In particular, a complete classification is achieved for those rings constructed using our method and elementary abelian groups of odd prime square order. It should be noted

that our classification method does not use standard ring isomorphism, but a weaker equivalence relation, which is certainly more natural for our problem and may be significant in the study of non-associative commutative rings in general.

In this article, rings are not assumed to be associative, nor to contain an identity. In general, the multiplication of a ring $\mathscr{R} = \{G, +, \cdot\}$ can be viewed as a bivariate function defined on the group $G = \{G, +\}$, which is both left and right distributive. It is easily seen that, given any ring $\mathscr{R}$ and any bivariate function $L(x, y)$ defined on $G \times G$ which satisfies

$$L(x + y, z) = L(x, z) + L(y, z) \quad \text{and} \quad L(x, y + z) = L(x, y) + L(x, z)$$

for all $x, y, z \in G$, it is possible to define a multiplication $\star$ on $G \times G$ by

$$x \star y = L(x, y)$$

resulting in a, possibly new, ring $\{G, +, \star\}$.

We now let $G = \{G, +\}$ be an abelian group and define an additional operation on G by constructing a function L as above, but by using a univariate function. Let $f : G \to G$ be any function. Define $\star_f$ on $G \times G$ by

$$x \star_f y = f(x + y) - f(x) - f(y)$$

for all $x, y \in G$. Note that $\star_f$ is commutative since G is assumed to be abelian. The definition can be extended to non-abelian groups using $x \star_f y = -f(x) + f(x + y) - f(y)$, but we do not consider them in the current article. This definition is motivated by results concerning planar functions in projective geometry, see [9], and we return to this topic in Section 5.

A natural question is when does $\{G, +, \star_f\}$ define a ring? An example can be seen through reverse engineering: let $\mathscr{R} = \{G, +, \cdot\}$ be a commutative ring with identity e in which $e + e = 2e$ is a unit. Then the function f given by $f : x \mapsto (2e)^{-1} \cdot x \cdot x$ defines a ring $\mathscr{R}_f = \{G, +, \star_f\}$ with $\mathscr{R}_f = \mathscr{R}$.

We give necessary and sufficient conditions on the function f so that $\{G, +, \star_f\}$ defines a ring. Further, we classify all functions which extend an elementary abelian p-group G to a ring.

Following this, we define weak isomorphism, a concept which sits between isomorphism of ring theory and isotopism of projective geometry. As with isomorphism and isotopism, weak isomorphism is an equivalence relation and in the context of our construction, appears to be the most natural and useful one to consider. We show there are precisely six non-weakly isomorphic classes of rings constructed using our method when $G = C_p \oplus C_p$ with p an odd prime. Thus the number of non-weakly isomorphic rings in this case is independent of p. It can be shown that this is not the case with the usual ring isomorphism.

We end the article by using our results to show that the only planar Dembowski-Ostrom polynomials over $\mathbb{F}_{p^2}$ are precisely those which can be written in the form $L_1(L_2^2(X))$ where L_1 and L_2 are linearised permutation polynomials.

2. Extending abelian groups to rings

Throughout this article, G denotes an abelian group written additively. For any integer $n \geq 1$ and any $a \in G$ we write na as the addition of n copies of a. By a *ring* $\mathscr{R} = \{G, +, \cdot\}$ we mean $(G, +)$ is an abelian group and

(i) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, and
(ii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,

for all $a, b, c \in G$.

For any function $f : G \to G$, define the difference operator $\star_f$ of f on G by

$$\star_f(x, y) = x \star_f y = f(x + y) - f(x) - f(y)$$

for all $x, y \in G$.

We view the operator $\star_f$ as a type of multiplication on G and note that it is necessarily commutative by definition. We now consider properties of $\{G, +, \star_f\}$. The following result is immediate.

THEOREM 2.1. *$\mathscr{R}_f = \{G, +, \star_f\}$ is a ring if and only if*

$$f(a + b + c) = f(a + b) + f(a + c) + f(b + c) - f(a) - f(b) - f(c) \tag{2.1}$$

holds for all $a, b, c \in G$.

PROOF. Left distributivity follows from the definition, and right distributivity by commutativity. □

In general, such a ring will have zero-divisors as $a \star_f b = 0$ precisely when $f(a + b) = f(a) + f(b)$. The example given in the introduction shows there are many rings which can be constructed in this way.

THEOREM 2.2. *Let $\{\mathscr{R}_f, +, \star_f\}$ be a ring. Then the following statements hold.*

(i) $f(0) = 0$.
(ii) $a \star_f 0 = 0 \star_f a = 0$ *for all* $a \in G$.
(iii) $a \star_f (-b) = (-a) \star_f b = -(a \star_f b)$ *for all* $a, b \in G$.
(iv) $(-a) \star_f (-b) = a \star_f b$ *for all* $a, b \in G$.

PROOF. For (i), set $a = b = c = 0$ in (2.1). The definition of $\star_f$ along with (i) yields (ii). By (2.1),

$$f(a) = f(a + b + (-b)) = f(a + b) + f(a - b) - f(a) - f(b) - f(-b)$$

so that

$$\begin{aligned} a \star_f (-b) &= f(a - b) - f(a) - f(-b) \\ &= -f(a + b) + f(a) + f(b) = -(a \star_f b). \end{aligned}$$

Similarly, $(-a) \star_f b = -(a \star_f b)$, yielding (iii), while (iv) is immediate from (iii). □

Recall that two rings $\mathscr{R}$ and $\mathscr{S}$ are isomorphic if there exists a bijective mapping $\phi : \mathscr{R} \to \mathscr{S}$ satisfying (i) $\phi(x + y) = \phi(x) + \phi(y)$, and (ii) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathscr{R}$.

THEOREM 2.3. *Let $\mathscr{R}_f = \{G, +, \star_f\}$ and $\mathscr{R}_h = \{G, +, \star_h\}$ be rings determined by the two functions f and h on G, respectively. Then $\mathscr{R}_f$ and $\mathscr{R}_h$ are isomorphic if and only if there exists a group automorphism ϕ on $\{G, +\}$ such that $x \star_{f\circ\phi} y = x \star_{\phi\circ h} y$ for all $x, y \in G$.*

PROOF. For any automorphism ϕ on $\{G, +\}$, we have

$$\begin{aligned} \phi(x) \star_f \phi(y) &= f(\phi(x) + \phi(y)) - f(\phi(x)) - f(\phi(y)) \\ &= f(\phi(x + y)) - f(\phi(x)) - f(\phi(y)) = x \star_{f\circ\phi} y, \end{aligned}$$

and

$$\begin{aligned} \phi(x \star_h y) &= \phi(h(x + y) - h(x) - h(y)) \\ &= \phi(h(x + y)) - \phi(h(x)) - \phi(h(y)) = x \star_{\phi\circ h} y. \end{aligned}$$

If $\mathscr{R}_f$ and $\mathscr{R}_h$ are isomorphic, then there exists an automorphism ϕ on $\{G, +\}$ such that $\phi(x) \star_f \phi(y) = \phi(x \star_h y)$, and so $x \star_{f\circ\phi} y = x \star_{\phi\circ h} y$ for all $x, y \in G$. Conversely, if there exists a group automorphism ϕ on $\{G, +\}$ such that $x \star_{f\circ\phi} y = x \star_{\phi\circ h} y$ for all $x, y \in G$, then clearly $\phi(x) \star_f \phi(y) = \phi(x \star_h y)$ and $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in G$, and so $\mathscr{R}_f$ and $\mathscr{R}_h$ are isomorphic. □

LEMMA 2.4. *Let $\mathscr{R}_f = \{G, +, \star_f\}$ and $\mathscr{R}_h = \{G, +, \star_h\}$ be rings determined by the two functions f and h on G, respectively. Then $\mathscr{R}_f = \mathscr{R}_h$ if and only if $f - h$ is a group homomorphism on G.*

PROOF. As both rings have the same additive group, we need only show that their multiplication operations are identical. Define $\psi(x) = f(x) - h(x)$. Then ψ is a group homomorphism on G if and only if, for all $x, y \in G$, $\psi(x + y) = \psi(x) + \psi(y)$, or

equivalently, $f(x+y)-h(x+y) = f(x)-h(x)+f(y)-h(y)$. Therefore ψ is a group homomorphism on G if and only if $f(x+y)-f(x)-f(y) = h(x+y)-h(x)-h(y)$. In other words, the multiplication operations $\star_f$ and $\star_h$ are the same. □

The example given in the introduction coupled with the previous lemma yields the following corollary.

COROLLARY 2.5. *Let $\mathscr{R} = \{G, +, \cdot\}$ be a commutative ring with identity ϵ and such that 2ϵ is a unit in $\mathscr{R}$. Then $\mathscr{R}_f = \{G, +, \star_f\} = \mathscr{R}$ if and only if $f : x \mapsto ((2\epsilon)^{-1} \cdot x \cdot x) + \phi(x)$ where ϕ is a group homomorphism on G.*

LEMMA 2.6. *Let $\mathscr{R}_f = \{G, +, \star_f\}$ be a ring with identity ϵ. Then*

(i) $\epsilon = f(\epsilon) + f(-\epsilon)$.

(ii) *For any integer $n \geq 1$, $f(n\epsilon) = nf(\epsilon) + (n(n-1)/2)\epsilon$.*

PROOF. We have $x = x \star_f \epsilon = f(x+\epsilon) - f(x) - f(\epsilon)$ for all $x \in G$. Setting $x = -\epsilon$ gives (i). An equivalent equation is

$$f(x+\epsilon) = x + f(x) + f(\epsilon). \tag{2.2}$$

If $x = \epsilon$, then $f(2\epsilon) = 2f(\epsilon) + \epsilon$. We proceed by induction. Suppose $f(n\epsilon) = nf(\epsilon) + (n(n-1)/2)\epsilon$ holds for some integer $n \geq 1$. Using (2.2), we have

$$\begin{aligned} f((n+1)\epsilon) &= n\epsilon + f(\epsilon) + f(n\epsilon) \\ &= n\epsilon + f(\epsilon) + nf(\epsilon) + (n(n-1)/2)\epsilon \\ &= (n+1)f(\epsilon) + (n(n+1)/2)\epsilon. \end{aligned}$$

Thus (ii) follows by induction. □

COROLLARY 2.7. *Let $G = \langle g \rangle$ be a finite cyclic group and $\mathscr{R}_f = \{G, +, \star_f\}$ define a ring with identity g. Then $|G|$ is odd.*

PROOF. Let $|G| = k$ be even. Then $ka = 0$ for all $a \in G$. By Lemma 2.6 (ii), $f(kg) = kf(g) + (k(k-1)/2)g = 0 + (k/2)(k-1)g \neq 0$ contradicting Theorem 2.2 (i). □

3. Extending elementary abelian groups to rings

For the remainder of the article we let G be an elementary abelian p-group of order $q = p^n$ with p a prime and n a positive integer. It is immediate that we can extend G

to a finite field and by Lagrange interpolation we can associate the function f on G with a unique polynomial f of degree less than q on the finite field of q elements. The key result of this section is Theorem 3.3, which for this case classifies those functions which extend G to a ring.

Before continuing we require some additional notation and definitions pertaining to finite fields. Further details can be found in [15]. We denote the finite field of q elements by $\mathbb{F}_q$ and the non-zero elements by $\mathbb{F}_q^*$. The symbol g will always represent a primitive element of $\mathbb{F}_q$. The ring of polynomials in indeterminate X will be denoted by $\mathbb{F}_q[X]$. We define the difference operator of a polynomial $f \in \mathbb{F}_q[X]$ to be the bivariate polynomial $\Delta_f(X, Y) = f(X+Y) - f(X) - f(Y)$ and identify the polynomial $\Delta_f(X, Y)$ with the bivariate function $\star_f$. For polynomials f_1, f_2, we write $f_1(f_2) = f_1 \circ f_2$ for the composition of f_1 with f_2. Recall a *permutation polynomial* over $\mathbb{F}_q$ is any polynomial that permutes the elements of $\mathbb{F}_q$ under evaluation.

A linear transformation over $\mathbb{F}_q$ can be described by a polynomial $L \in \mathbb{F}_q[X]$, called a *p-polynomial* (also known as a linearised or additive polynomial), with shape $L(X) = \sum_{i=0}^{n-1} a_i X^{p^i}$. Any p-polynomial L satisfies $L(x+y) = L(x) + L(y)$ and $L(ax) = aL(x)$ for all $x, y \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$. It is immediate from the first of these two properties that L is a permutation polynomial over $\mathbb{F}_q$ if and only if $x = 0$ is the only root of L in $\mathbb{F}_q$.

A particularly important p-polynomial is the *absolute trace mapping*, denoted Tr, which is defined to be the polynomial

$$\mathrm{Tr}(X) = \sum_{i=0}^{n-1} X^{p^i}.$$

A key property of the trace mapping is $\mathrm{Tr}(x) \in \mathbb{F}_p$ for all $x \in \mathbb{F}_q$. The trace mapping is also equidistributive by which we mean that every element $a \in \mathbb{F}_p$ has p^{n-1} pre-images.

The set of all p-polynomials which are permutations over $\mathbb{F}_q$ form a group, under composition modulo $X^q - X$, isomorphic to the general linear group $\mathrm{GL}(n, p)$. We shall denote this group by $\mathscr{G}$ throughout. For notational simplicity, we write $L \in \mathscr{G}$ to mean $L \in \mathbb{F}_q[X]$ is a permutation polynomial. For the following result, see [15, Chapter 7].

LEMMA 3.1. *The polynomial $L(X) = aX^q + bX \in \mathbb{F}_{q^2}[X]$ is a permutation polynomial over $\mathbb{F}_{q^2}$ if and only if $a^{q+1} \neq b^{q+1}$.*

A *Dembowski-Ostrom* (DO) polynomial is any polynomial $f \in \mathbb{F}_q[X]$ of the shape

$$f(X) = \sum_{i,j=0}^{n-1} a_{ij} X^{p^i + p^j}.$$

More precisely, we shall call f a p^s-DO polynomial if $a_{ij} = 0$ whenever i or j are not divisible by s. DO polynomials play a key role in the study of planar functions; see Section 5. The following result characterises DO polynomials in terms of their difference operator.

THEOREM 3.2. *Let $f \in \mathbb{F}_q[X]$ with $\deg(f) < q$. Then the following conditions are equivalent.*

(i) *$f = D + L$, where D is a Dembowski-Ostrom polynomial and L is a p-polynomial.*

(ii) *For each $a \in \mathbb{F}_q^*$, $\Delta_f(X, a) = L_a(X)$ where L_a is a p-polynomial depending on a.*

For the proof, see [7, Theorem 3.2]. The statement of this result differs slightly from that given in [7] because we are dealing with a different definition of the difference operator. However, it is easily seen that the proof as given there suffices.

We now classify those functions which extend an elementary abelian p-group to a ring.

THEOREM 3.3. *Let G be an elementary abelian p-group and $f \in \mathbb{F}_q[X]$. Then $\mathscr{R}_f = \{G, +, \star_f\}$ is a ring if and only if f satisfies $f(X) = D(X) + L(X)$ where D is a DO polynomial and L is a p-polynomial.*

PROOF. Let $f \in \mathbb{F}_q[X]$ satisfy $f(X) = D(X) + L(X)$. Now Δ_f is symmetric in X and Y. It follows from Theorem 3.2 that $\Delta_f(X, Y)$ is a p-polynomial in both X and Y. In particular, we have $\Delta_f(a + b, c) = \Delta(a, c) + \Delta(b, c)$ for all $a, b, c \in \mathbb{F}_q$. Hence Δ_f yields both distributive laws, and so $\mathscr{R}_f$ is a ring. Now suppose $\mathscr{R}_f$ is a ring. Then $\star_f$ and hence Δ_f are left and right distributive as mappings. Thus $\Delta_f(X, a)$ must be a p-polynomial for all $a \in \mathbb{F}_q^*$. By Theorem 3.2, $f(X) = D(X) + L(X)$ for some DO polynomial D and some p-polynomial L. □

We now consider an example. Let $q = p^n$ with n a positive integer and define $f(X) = X^{p^\alpha+1}$ where $\alpha \geq 0$. It is easy to see that $\Delta_f(X, Y) = X^{p^\alpha}Y + XY^{p^\alpha} = X \star_f Y$. For $x, y, z \in \mathbb{F}_q^*$, a short calculation reveals

$$(x \star_f y) \star_f z = x^{p^{2\alpha}} y^{p^\alpha} z + x^{p^\alpha} y^{p^{2\alpha}} z + x^{p^\alpha} y z^{p^\alpha} + x y^{p^\alpha} z^{p^\alpha}$$
$$x \star_f (y \star_f z), = x^{p^\alpha} y^{p^\alpha} z + x^{p^\alpha} y z^{p^\alpha} + x y^{p^{2\alpha}} z^{p^\alpha} + x y^{p^\alpha} z^{p^{2\alpha}}.$$

Suppose $\mathscr{R}_f$ is associative. Fix $x, y \in \mathbb{F}_q^*$ and consider the two multiplications above as polynomials in the indeterminate Z by replacing z with Z. Then the two polynomials, one of degree p^α and one of degree $p^{2\alpha}$, are identical under evaluation,

which is impossible unless $\alpha \equiv 0 \bmod n$ or $n = 2$. If $n = 2$, then the two polynomials become (under reduction modulo $Z^{p^2} - Z$)

$$(x \star_f y) \star_f Z = (Z + Z^{p^\alpha})(xy^{p^\alpha} + x^{p^\alpha} y),$$
$$x \star_f (y \star_f Z) = Z(x^{p^\alpha} y^{p^\alpha} + xy^{p^\alpha}) + Z^{p^\alpha}(x^{p^\alpha} y + xy).$$

It follows that $y = y^{p^\alpha}$ for all $y \in \mathbb{F}_{p^2}$, implying $\alpha \equiv 0 \bmod n$. Thus $\mathscr{R}_f$ is an associative ring if and only if $\alpha \equiv 0 \bmod n$, in which case $f(X) \bmod (X^q - X) = kX^2$ for some $k \in \mathbb{F}_q$. A similar argument shows that $\mathscr{R}_f$ has a multiplicative identity ϵ if and only if $\alpha \equiv 0 \bmod n$.

It is not true in general that $\mathscr{R}_f$ has a multiplicative identity if and only if $f(X) \equiv kX^2 \bmod (X^q - X)$. For example, the ring $\mathscr{R}_f$ with DO polynomial $f(X) = X^2 + 2X^{p^2+p} - X^{2p} - X^{2p^2}$ has multiplicative identity $\epsilon = (p+1)/2$ over any finite field $\mathbb{F}_{p^n}$, p odd.

It is also the case, for $f = D + L$ as in Theorem 3.3, that if $\mathscr{R}_f$ has an identity ϵ, then it is a root of the polynomial $D(X) - X$, by Lemma 2.6 (i).

4. The number of non-equivalent rings

Our next objective is to describe machinery that allows us to determine if two rings constructed from the same elementary abelian group, but using different DO polynomials, are equivalent. As an application, we show that relevant to weak isomorphism (defined below) there are six distinct rings of odd order p^2 constructed in this way (effectively there is only one DO polynomial, X^3, to consider over $\mathbb{F}_{2^2}$).

The class of DO polynomials is closed under composition with p-polynomials. In particular, one can define an equivalence relation on DO polynomials in the following manner: two DO polynomials f_1, f_2 are called equivalent, written $f_1 \sim f_2$, if there exist $L_1, L_2 \in \mathscr{G}$ such that $L_1 \circ f_1 \circ L_2 \equiv f_2 \bmod (X^q - X)$. Generally, we make use of the equivalent statement: $f_1 \sim f_2$ if there exist $L_1, L_2 \in \mathscr{G}$ such that

$$L_1 \circ f_1 \equiv f_2 \circ L_2 \bmod (X^q - X).$$

This equivalence relation can be defined more generally, both in the choice of the group G and for all polynomials over $\mathbb{F}_q$. It appears the study of such equivalence relations and the related problem of modular invariants began with Dickson in [10], and has since been taken up in various forms by Carlitz, [1, 2], Cavior, [3, 4], and Mullen [16, 17, 18].

For two DO polynomials $f, h \in \mathbb{F}_q[X]$, we shall call the rings $\mathscr{R}_f = \{\mathbb{F}_q, +, \star_f\}$ and $\mathscr{R}_h = \{\mathbb{F}_q, +, \star_h\}$ *weakly isomorphic* if there exist two linear transformations $L_1, L_2 \in \mathscr{G}$ such that $L_1(x) \star_f L_1(y) = L_2(x \star_h y)$ for all $x, y \in \mathbb{F}_q$. This lies between

the concept of ring isomorphism, see [12, page 133], and the concept of semifield isotopism, see [8, page 135]. This definition could be extended to general rings, but we will not need it here. This definition is motivated by the equivalence relation for DO polynomials, as illustrated in our next result. The proof is trivial.

LEMMA 4.1. *Let $f, h \in \mathbb{F}_q[X]$ be DO polynomials. The rings $\mathscr{R}_f$ and $\mathscr{R}_h$ are weakly isomorphic if and only if there exist $L_1, L_2 \in \mathscr{G}$ such that $f = L_1 \circ h \circ L_2 \bmod (X^q - X)$.*

Let $q = p^n$ and set $d < n$ to be a positive divisor of n. Suppose $f \in \mathbb{F}_q[X]$ is a DO polynomial such that $f(X) \equiv cX^2 \bmod (X^{p^d} - X)$, for some $c \in \mathbb{F}_q^*$. This can happen if and only if f is a p^d-DO polynomial. So $\mathscr{R}_f$ contains a weakly isomorphic copy of $\mathbb{F}_{p^d}$. In particular, for any DO polynomial f, the ring $\mathscr{R}_f$ must contain a weakly homomorphic copy of $\mathbb{F}_p$. More precisely, $f(X) \bmod (X^p - X) = cX^2$ for some $c \in \mathbb{F}_q$ and if $c \neq 0$, then $\mathscr{R}_f$ contains a weakly isomorphic copy of $\mathbb{F}_p$. Otherwise $x \star_f y = 0$ for all $x, y \in \mathbb{F}_p$.

A *weak automorphism* of a polynomial f is a pair of polynomials $(L_1, L_2) \in \mathscr{G} \times \mathscr{G}$ such that $L_1 \circ f \equiv f \circ L_2 \bmod (X^q - X)$. The set $\Omega(f)$ of all weak automorphisms of f forms a group under the operation of pairwise composition: $(L_1, L_2) \cdot (M_1, M_2) = (L_1 \circ M_1, L_2 \circ M_2)$. More importantly, the cardinality of $\Omega(f)$ is invariant for polynomials f in the same equivalence class. An application of [18, Theorem 2.4] yields the following lemma.

LEMMA 4.2. *Let $\Omega(f)$ denote the group of weak automorphisms of the DO polynomial f and let $C(f)$ denote the equivalence class containing f. Then*

$$|C(f)| = \frac{|\mathscr{G}|^2}{|\Omega(f)|}.$$

We now restrict ourselves specifically to the case where the elementary abelian p-group G has odd order p^2. Our aim is to determine the number of non-weakly isomorphic rings which can be constructed from G using our method. We take a constructive approach and determine a DO polynomial which acts as the class representative for each class as well as the number of elements in each class. To determine the number of elements in each class we use the result of Mullen from [18] (given above as Lemma 4.2), and determine the number of weak automorphisms of each polynomial instead. The following lemma will be used extensively in what follows. The proof is purely mechanical and so we omit it.

LEMMA 4.3. *Let $L_1(X) = aX^p + bX$ and $L_2(X) = cX^p + dX$ with $a, b, c, d \in \mathbb{F}_q$. Define $f(X) = \alpha X^2 + \beta X^{p+1} + \gamma X^{2p}$ to be a general DO polynomial defined over*

$\mathbb{F}_{p^2}$. *Then we have*

$$\begin{aligned} &L_1(X) \circ f(X) \bmod (X^{p^2} - X) \\ &\quad = (a\gamma^p + b\alpha)X^2 + (a\beta^p + b\beta)X^{p+1} + (a\alpha^p + b\gamma)X^{2p} \end{aligned}$$

and

$$\begin{aligned} &f(X) \circ L_2(X) \bmod (X^{p^2} - X) \\ &\quad = (\alpha d^2 + \beta c^p d + \gamma c^{2p})X^2 + (2\alpha cd + \beta(c^{p+1} + d^{p+1}) + 2\gamma c^p d^p)X^{p+1} \\ &\qquad + (\alpha c^2 + \beta d^p c + \gamma d^{2p})X^{2p}. \end{aligned}$$

4.1. Equivalence classes of DO monomials We first consider the equivalence classes containing the DO monomials. For $\mathbb{F}_{p^2}$ there are only three DO monomials: X^2, X^{p+1} and X^{2p}. Clearly $X^{2p} \in C(X^2)$.

LEMMA 4.4. *We have* $|\Omega(X^2)| = 2(p^2 - 1)$ *and* $|\Omega(X^{p+1})| = 2p(p-1)(p^2-1)$.

PROOF. Set $f(X) = X^2$. We need to determine the number of pairs $(L_1, L_2) \in \mathscr{G} \times \mathscr{G}$ such that $L_1 \circ f \equiv f \circ L_2 \bmod (X^q - X)$. Using Lemma 4.3 and equating terms we have the three equations

$$a = c^2, \quad 0 = 2cd, \quad b = d^2.$$

Thus $cd = 0$, from which it follows that L_1 and L_2 are necessarily monomials. In fact, either $a = c^2$ and $b = d = 0$, or $b = d^2$ and $a = c = 0$, and

$$\Omega(X^2) = \{(c^2X^p, cX^p) \mid c \in \mathbb{F}_{p^2}^*\} \cup \{(d^2X, dX) \mid d \in \mathbb{F}_{p^2}^*\}.$$

Thus $|\Omega(X^2)| = 2(p^2 - 1)$.

Now let $f(X) = X^{p+1}$. From Lemma 4.3, we again obtain three equations:

$$0 = cd^p, \quad a + b = c^{p+1} + d^{p+1}, \quad 0 = c^p d.$$

So $cd = 0$ and either $c = 0$ and $a + b = d^{p+1}$, or $d = 0$ and $a + b = c^{p+1}$. As the cases are symmetric, we count only for the second case. There are $p^2 - 1$ choices of $c \neq 0$. In each case $c^{p+1} \in \mathbb{F}_p^*$. For every $a \in \mathbb{F}_{p^2}$, there is exactly one choice of b such that $a + b = c^{p+1}$. However, we need to test that $L_1(X) = aX^p + bX$ is invertible as well. With $b = c^{p+1} - a$, L_1 is not invertible if and only if $a^p + a = c^{p+1}$; see Lemma 3.1. As the trace mapping Tr is equidistributive, there are exactly p choices of a for each chosen c such that L_1 is not invertible. Hence, there are $p^2 - 1$ choices for c and $p^2 - p$ choices for a. Including the symmetry, we have shown that $|\Omega(X^{p+1})| = 2p(p-1)(p^2-1)$ as required. □

4.2. Equivalence classes of DO binomials We now deal with two DO binomials: $X^{p+1} + X^2$, and $X^{2p} - X^2$. By determining the number of weak automorphisms for each of these binomials, we shall show that they cannot be equivalent to each other, or to the two monomial classes of the previous section.

LEMMA 4.5. *We have*

$$|\Omega(X^{p+1} + X^2)| = p(p-1)^2 \quad \textit{and} \quad |\Omega(X^{2p} - X^2)| = 2p(p-1)^3.$$

PROOF. Setting $f(X) = X^{p+1} + X^2$, and applying Lemma 4.3, we obtain the three equations

$$a = c^2 + cd^p, \tag{4.1}$$

$$a + b = 2cd + c^{p+1} + d^{p+1}, \tag{4.2}$$

$$b = d^2 + c^p d. \tag{4.3}$$

Adding (4.1) to (4.3) and equating the result with (4.2) eventually gives

$$(c-d)^2 = (c-d)^{p+1}.$$

It follows that $c - d \in \mathbb{F}_p^*$ (as we may omit $c = d$). Substituting $d^p = c^p - c + d$ into (4.3) we obtain $a = c^{p+1} + cd$. A similar calculation with (4.1) gives $b = d^{p+1} + cd$. Now taking the last two equations and subtracting one from the other shows

$$a - b = c^{p+1} - d^{p+1} \tag{4.4}$$

implying $a - b \in \mathbb{F}_p^*$. We shall now show that $a^{p+1} = b^{p+1}$ implies $c^{p+1} = d^{p+1}$. We have $a^p - b^p = a - b$. Multiplying through by a and assuming $a^{p+1} = b^{p+1}$ we obtain the equation

$$(b^p + a)(b - a) = 0.$$

If $a = b$, then (4.4) implies $c^{p+1} = d^{p+1}$. If $a = -b^p$, then using (4.1) and (4.3) we have $(c^p + d)^2 = 0$, or $c^p = -d$. It follows that $c^{p+1} = -cd = d^{p+1}$. It remains to count the pairs (c, d) satisfying $c - d \in \mathbb{F}_p^*$ and $c^{p+1} \neq d^{p+1}$. There are p^2 choices for c. For each c there are $p - 1$ choices for d such that $c - d \in \mathbb{F}_p^*$. This gives $p^2(p-1)$ pairs overall. We need to remove those pairs where $c^{p+1} = d^{p+1}$. Assume $c^{p+1} = d^{p+1}$. We have $(c-d)^p = c - d$. Multiplying through by c yields the equation

$$(d^p + c)(d - c) = 0.$$

So either $d = c$ or $d = -c^p$. If $\mathrm{Tr}(c) = c^p + c = 0$, then there is only one choice of d for which $c^{p+1} = d^{p+1}$ (as $c = -c^p$). If $\mathrm{Tr}(c) \neq 0$, then there are two

choices. We must therefore remove p pairs for the case $\mathrm{Tr}(c) = 0$ (as there are p such $c \in \mathbb{F}_{p^2}$), and $2(p^2 - p)$ pairs for the case $\mathrm{Tr}(c) \neq 0$. This means that there are $p^2(p-1) - 2p(p-1) - p = p(p-1)^2$ legitimate pairs (c, d), and as a and b are fixed by c and d, there are $p(p-1)^2$ weak automorphisms of $X^{p+1} + X^2$.

For $f(X) = X^{2p} - X^2$, Lemma 4.3 yields the equations

$$a - b = c^{2p} - d^2, \tag{4.5}$$

$$0 = 2(cd)^p - 2cd, \tag{4.6}$$

$$b - a = d^{2p} - c^2. \tag{4.7}$$

Raising (4.5) to the power p and using (4.7) shows $a - b \in \mathbb{F}_p$. Equation (4.6) shows $cd \in \mathbb{F}_p$. Also, equating (4.5) and (4.7) shows $c^2 + d^2 \in \mathbb{F}_p$. If $cd \neq 0$, then $(c^2 + d^2)/cd \in \mathbb{F}_p$. Setting $\eta = c/d$, we have

$$\eta^p + \eta^{-p} = \eta + \eta^{-1}$$

from which it follows $(\eta^{p+1} - 1)(\eta^{p-1} - 1) = 0$. So $c^{p+1} = d^{p+1}$ or $c/d \in \mathbb{F}_p$. As we can exclude the first possibility, it follows that $c^2, d^2 \in \mathbb{F}_p$ (even if $cd = 0$). We thus have the following relevant conditions:

$$c^2, d^2 \in \mathbb{F}_p, \tag{4.8}$$

$$cd \in \mathbb{F}_p, \tag{4.9}$$

$$a - b \in \mathbb{F}_p^*. \tag{4.10}$$

To begin counting, if $c = 0$, then $d = g^{i(p+1)/2}$, with $0 \leq i < 2(p-1)$. So there are $2(p-1)$ choices for d when $c = 0$. Likewise, when $d = 0$ we have $2(p-1)$ choices for c. Overall we have $4(p-1)$ choices for pairs (c, d) when $cd = 0$. When $cd \neq 0$, we have $2(p-1)$ choices for c $\left(= g^{i(p+1)/2}\right)$. We require $d^2, cd \in \mathbb{F}_p^*$, and $d^{p+1} \neq c^{p+1}$. Conditions (4.8) and (4.9) imply $d = g^{j(p+1)/2}$ where $0 \leq j < 2(p-1)$ and $i \equiv j \bmod 2$. There are $p - 1$ such d. However, two such choices will give $c^{p+1} = d^{p+1}$ (they are $d = c$ or $d = -c$). So there are $p - 3$ legitimate choices for d. Overall we have $2(p-1)(p-3) + 4(p-1) = 2(p-1)^2$ choices for pairs (c, d). For these pairs (c, d), choosing an $a \in \mathbb{F}_{p^2}$ fixes b. We are left to determine the number of $a \in \mathbb{F}_{p^2}$ such that $a^{p+1} \neq b^{p+1}$ where $a - b \in \mathbb{F}_p$. We have $b = a + \alpha$, where $\alpha \in \mathbb{F}_p^*$. A short calculation yields

$$b^{p+1} = a^{p+1} + \alpha(\alpha + \mathrm{Tr}(a)).$$

Suppose $a^{p+1} = b^{p+1}$. Then $\mathrm{Tr}(a) = -\alpha$ and there are p choices for $a \in \mathbb{F}_{p^2}$ such that this holds. Therefore there are $p^2 - p$ choices for a (and hence pairs (a, b)). In summary, there are $(p^2 - p)(2(p-1)^2) = 2p(p-1)^3$ weak automorphisms of the polynomial $X^{2p} - X^2$. □

The equation involving $\eta + \eta^{-1}$ in the last argument will be familiar to those who have studied the Dickson Polynomials of the first and second kind, see [14].

4.3. Equivalence classes of DO trinomials It remains to consider two final classes, both of which are generated by DO trinomials. In the next section we shall show that we have exhausted the number of classes.

LEMMA 4.6. *We have*

$$|\Omega(X^{2p} - 2X^{p+1} + X^2)| = p^2(p-1)^3 \quad \textit{and}$$
$$|\Omega(X^{2p} + gX^{p+1} + X^2)| = 2(p-1)^2.$$

PROOF. Let $f(X) = X^{2p} - 2X^{p+1} + X^2$. Applying Lemma 4.3 yields

$$a + b = d^2 - 2c^p d + c^{2p} = (c^p - d)^2, \tag{4.11}$$
$$a + b = c^{p+1} + d^{p+1} - cd - (cd)^p = (c^p - d)(c - d^p), \tag{4.12}$$
$$a + b = c^2 - 2cd^p + d^{2p} = (c - d^p)^2. \tag{4.13}$$

Equating (4.11) and (4.12), we have either $c + d \in \mathbb{F}_p$ or $c^p = d$. However, $c^p = d$ implies $c + d \in \mathbb{F}_p$. We also have $a + b \in \mathbb{F}_p$ as (4.12) is unaltered by taking pth powers. The count for pairs (c, d) follows in exactly the same fashion as for $f(X) = X^{p+1} + X^2$, resulting in $p(p-1)^2$ pairs. The calculation for pairs (a, b) is exactly the same as it was for the case $f(X) = X^{2p} - X^2$, giving $p^2 - p$ such pairs. Thus $|\Omega(X^{2p} - 2X^{p+1} + X^2)| = p^2(p-1)^3$.

Now set $f(X) = X^{2p} + gX^{p+1} + X^2$. From Lemma 4.3, the following three equations must be satisfied.

$$a + b = d^2 + gc^p d + c^{2p}, \tag{4.14}$$
$$g^p a + gb = g(c^{p+1} + d^{p+1}) + 2cd + 2(cd)^p, \tag{4.15}$$
$$a + b = c^2 + gcd^p + d^{2p}. \tag{4.16}$$

From (4.14), we have

$$(a+b)^p + (a+b) = c^{2p} + c^2 + d^{2p} + d^2 + g^p cd^p + gc^p d.$$

Likewise, (4.16) yields

$$(a+b)^p + (a+b) = c^{2p} + c^2 + d^{2p} + d^2 + g^p c^p d + gcd^p.$$

Equating these shows that $c^p d \in \mathbb{F}_p$.

Returning to (4.14) and (4.16), we have $c^2 - d^2 \in \mathbb{F}_p$. If $cd \neq 0$, then

$$c^2 - d^2 = c^{2p} - d^{2p} = c^{2p} - c^{-2}(c^p d)^2 = c^{2p-2}(c^2 - d^2).$$

If $c^2 = d^2$, then $c^{p+1} = d^{p+1}$, a case we must exclude. It follows that $c^2, d^2 \in \mathbb{F}_p$ (regardless of whether $cd = 0$ or not). These are almost the same conditions for c, d as in the case $f(X) = X^{2p} - X^2$ (replace $cd \in \mathbb{F}_p$ with $c^p d \in \mathbb{F}_p$). A similar counting argument can be used, giving $2(p-1)^2$ pairs (c, d). It remains to show that a and b are completely determined by c and d, and that $a^{p+1} \neq b^{p+1}$ holds whenever $c^{p+1} \neq d^{p+1}$. Equations (4.14)–(4.16) now generate

$$a + b = c^2 + d^2 + gc^p d, \tag{4.17}$$

$$ag^p + bg = g(c^{p+1} + d^{p+1}) + 2\,\mathrm{Tr}(cd). \tag{4.18}$$

Multiplying (4.17) by g and subtracting the result from (4.18) shows

$$(g^p - g)a = 2\,\mathrm{Tr}(cd) + g(c^{p+1} + d^{p+1} - c^2 - d^2) + g^2 c^p d.$$

So a is determined completely by c and d, which in turn implies b is also. Suppose $a^{p+1} = b^{p+1}$. We may assume $ab \neq 0$. Obviously

$$g^p(a^{p+1} - b^{p+1}) + a^p(bg - bg) = 0.$$

It follows that $a^p(ag^p + bg) - b(b^p g^p + a^p g) = 0$. Raising this to the power p and subtracting the result from the initial expression we obtain

$$(a + b)(ag^p + bg)^p - (a + b)^p(ag^p + bg) = 0. \tag{4.19}$$

Substituting into (4.19) using the values of $a + b$ and $ag^p + bg$ (and their pth powers) from (4.17) and (4.18), one obtains the equation

$$c^{p+3} + d^{p+3} - 2c^2 d^{p+1} = 0. \tag{4.20}$$

As $c^p d = cd^p$, (4.20) implies

$$(d^{p+1} - c^{p+1})(d^2 - c^2) = 0.$$

Thus $a^{p+1} = b^{p+1}$ implies $c^{p+1} = d^{p+1}$, which are the cases we have already excluded. Hence $|\Omega(X^{2p} + gX^{p+1} + X^2)| = 2(p-1)^2$. □

4.4. A complete set of equivalence classes We need to show that the six classes given in the previous three sections do indeed account for all DO polynomials over $\mathbb{F}_{p^2}$.

THEOREM 4.7. *Under weak equivalence, there are six equivalence classes of DO polynomials, and these are described by the six polynomials* X^2, X^{p+1}, $X^{p+1} + X^2$, $X^{2p} - X^2$, $X^{2p} - 2X^{p+1} + X^2$ *and* $X^{2p} + gX^{p+1} + X^2$.

PROOF. That the six polynomials given always describe different classes is easily established from noting that no two formulae for the number of weak automorphisms (as determined in the previous three sections) can be equal for a fixed prime $p > 2$.

It remains to show that these six classes contain all DO polynomials over $\mathbb{F}_{p^2}$. Let $f_1(X) = X^2$, $f_2(X) = X^{p+1}$, $f_3(X) = X^{p+1} + X^2$, $f_4(X) = X^{2p} - X^2$, $f_5(X) = X^{2p} - 2X^{p+1} + X^2$ and $f_6(X) = X^{2p} + gX^{p+1} + X^2$. There are $p^6 - 1$ DO polynomials over $\mathbb{F}_{p^2}$ (we exclude the zero polynomial). We need to show

$$p^6 - 1 = \sum_{i=1}^{6} |C(f_i)|.$$

Recall $|\mathscr{G}| = p(p-1)(p^2-1)$. By Lemma 4.2 and the results of the previous three sections, we have

$$|C(f_1)| = \left(\frac{p^2-1}{2}\right)(p^4 - 2p^3 + p^2), \qquad |C(f_2)| = \left(\frac{p^2-1}{2}\right)(p^2 - p),$$
$$|C(f_3)| = \left(\frac{p^2-1}{2}\right)(2p^3 - 2p), \qquad |C(f_4)| = \left(\frac{p^2-1}{2}\right)(p^2 + p),$$
$$|C(f_5)| = \left(\frac{p^2-1}{2}\right)(2p + 2), \qquad |C(f_6)| = \left(\frac{p^2-1}{2}\right)(p^4 - p^2).$$

Summing gives

$$\sum_{i=1}^{6} |C(f_i)| = \left(\frac{p^2-1}{2}\right)(2p^4 + 2p^2 + 2) = p^6 - 1$$

as required. □

Since two rings are weakly isomorphic if they are isomorphic, it is seen that this construction method yields at least six non-isomorphic rings of order p^2 for any odd prime p. Computational evidence leads us to make the following conjecture.

CONJECTURE 4.8. *Let p an odd prime. Then the number of non-isomorphic rings $\{\mathbb{F}_{p^2}, +, \star_f\}$ generated by polynomials $f \in \mathbb{F}_{p^2}[X]$ is $p^2 + 3p + 6$ if $p > 3$ and $p^2 + 3p + 5$ if $p = 3$.*

The method used above for weak isomorphism may be adapted for the isomorphism problem provided good class representatives can be found.

5. Planar functions

A polynomial f over $\mathbb{F}_q$ is *planar* if for every $a \in \mathbb{F}_q^*$, the polynomial $\Delta_f(X, a)$ is a permutation polynomial over $\mathbb{F}_q$. Planar functions have been used to construct

projective planes, see [9]. All planar DO polynomials necessarily describe semifield planes.

We end the article by applying our results to classify those DO polynomials which are planar over $\mathbb{F}_{p^2}$. By [7, Theorem 2.3], either every polynomial in a class is a planar function, or every polynomial in a class is not. So we need only test the planarity of the class representatives.

THEOREM 5.1. *A DO polynomial $f \in \mathbb{F}_{p^2}[X]$ is planar if and and only if $f(X) \equiv L_1(L_2^2(X)) \bmod (X^{p^2} - X)$, where $L_1, L_2 \in \mathscr{G}$.*

PROOF. It follows from [7, Theorem 3.3] that X^2 is planar and X^{p+1} is not planar. For the remaining class representatives, it is easy to show

$$\begin{aligned}
\Delta_{f_3}(X, a) &= aX^p + (a^p + 2a)X,\\
\Delta_{f_4}(X, a) &= 2((aX)^p - aX),\\
\Delta_{f_5}(X, a) &= 2((a^p - a)X^p - (a^p - a)X),\\
\Delta_{f_6}(X, a) &= (2a^p + ga)X^p + (2a + ga^p)X).
\end{aligned}$$

We proceed to show that each of these difference polynomials cannot be permutation polynomials of $\mathbb{F}_{p^2}$ for all $a \in \mathbb{F}_{p^2}^*$. Now $a^{p+1} - (a^p + 2a)^{p+1} = -2(a^p + a)^2 = -2\,\mathrm{Tr}(a)^2$. As the trace mapping is equidistributive, there are $p-1$ choices of $a \in \mathbb{F}_{p^2}^*$ such that $\mathrm{Tr}(a) = 0$ and $aX^p + (a^p + 2a)X$ is not a permutation polynomial (by Lemma 3.1). For any $a \in \mathbb{F}_{p^2}^*$, both $\Delta_{f_4}(X, a)$ and $\Delta_{f_5}(X, a)$ are permutation polynomials if and only if $X^p - X$ is. Since $X^p - X$ has p roots, $\Delta_{f_4}(X, a)$ and $\Delta_{f_5}(X, a)$ are never permutation polyonomials. Finally, for $a \in \mathbb{F}_p$, $(2a^p + ga)X^p + (2a + ga^p)X = a(2 + g)\,\mathrm{Tr}(X)$, which cannot be a permutation polynomial. Hence X^2 is the only class representative which is planar and every planar DO polynomial must be of the form $L_1 \circ X^2 \circ L_2 \bmod (X^{p^2} - X)$ with $L_1, L_2 \in \mathscr{G}$. □

It has been known for some time, see [13], that any semifield plane of order p^2 is desarguesian and that the class $C(X^2)$ describes the desarguesian plane, see [7, Theorem 5.2]. Thus Theorem 5.1 shows there are no other planar DO polynomials which describe the desarguesian plane of order p^2.

References

[1] L. Carlitz, 'Invariantive theory of equations in a finite field', *Trans. Amer. Math. Soc.* **75** (1953), 405–427.

[2] ———, 'Invariant theory of systems of equations in a finite field', *J. Analyse Math.* **3** (1954), 382–413.

[3] S. R. Cavior, 'Equivalence classes of functions over a finite field', *Acta Arith.* **10** (1964), 119–136.
[4] ———, 'Equivalence classes of sets of polynomials over a finite field', *J. Reine Angew. Math.* **225** (1967), 191–202.
[5] B. Corbas and G. D. Williams, 'Rings of order p^5. Part I. Nonlocal rings', *J. Algebra* **231** (2000), 677–690.
[6] ———, 'Rings of order p^5. Part II. Local rings', *J. Algebra* **231** (2000), 691–704.
[7] R. S. Coulter and R. W. Matthews, 'Planar functions and planes of Lenz-Barlotti class II', *Des. Codes Cryptogr.* **10** (1997), 167–184.
[8] P. Dembowski, *Finite geometries* (Springer, New York, 1968, reprinted 1997).
[9] P. Dembowski and T. G. Ostrom, 'Planes of order n with collineation groups of order n^2', *Math. Z.* **103** (1968), 239–258.
[10] L. E. Dickson, 'General theory of modular invariants', *Trans. Amer. Math. Soc.* **10** (1909), 123–158.
[11] E. G. Goodaire and Y. Zhou, 'Alternative rings of small order', *Comm. Algebra* **28** (2000), 3335–3349.
[12] I. N. Herstein, *Topics in algebra*, 2nd edition (John Wiley & Sons, 1975).
[13] D. E. Knuth, 'Finite semifields and projective planes', *J. Algebra* **2** (1965), 182–217.
[14] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Appl. Math. 65 (Longman Scientific and Technical, Essex, England, 1993).
[15] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., vol. 20 (Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press)).
[16] G. L. Mullen, 'Equivalence classes of functions over a finite field', *Acta Arith.* **29** (1976), 353–358.
[17] ———, 'Equivalence classes of polynomials over finite fields', *Acta Arith.* **31** (1976), 113–123.
[18] ———, 'Weak equivalence of functions over a finite field', *Acta Arith.* **35** (1979), 259–272.
[19] G. D. Williams, 'On a class of finite rings of characteristic p^2', *Result. Math.* **38** (2000), 377–390.

School of Computing and Mathematics
Deakin University
221 Burwood Highway
Burwood Vic 3125
Australia
e-mail: lmbatten@deakin.edu.au

Department of Mathematical Sciences
520 Ewing Hall
University of Delaware
Newark, Delaware 19716
USA
e-mail: coulter@math.udel.edu

307/60 Willis Street
Te Aro (Wellington), 6001
New Zealand
e-mail: marie.henderson@ssc.govt.nz