ACTA ARITHMETICA
112.4 (2004)

Explicit formulas for strong Davenport pairs

by

Antonia W. Bluher (Fort George G. Meade, MD)

1. Introduction. Let F be a finite field and $\overline{F}$ its algebraic closure. Two separable polynomials $g, h \in F[x]$ are said to be a *strong Davenport pair* if $g(K) = h(K)$ for all finite extensions K/F, where $g(K) = \{g(b) \mid b \in K\}$. We will say that g and h are *isovalent* if for any finite extension field K/F and any $a \in K$,

$$|g^{-1}(a) \cap K| = |h^{-1}(a) \cap K|.$$

Note that $a \in g(K)$ if and only if $g^{-1}(a) \cap K$ is nonempty, so if g, h are isovalent then they are a strong Davenport pair.

Let q be a power of $\mathrm{char}(F)$. We adopt the notation: $\langle j \rangle = (q^j - 1)/(q-1) \in \mathbb{Z}$ if $j \geq 0$. Then $\langle 0 \rangle = 0$, $\langle 1 \rangle = 1$, and $\langle j \rangle = 1 + q + q^2 + \ldots + q^{j-1}$ for $j \geq 2$. Note that $\langle n \rangle - \langle j \rangle = q^j \langle n - j \rangle$ when $n \geq j$. We now present our main result.

Theorem 1.1. *Let $n \geq 2$, $\delta_1, \ldots, \delta_{n-1} \in F$, and*

$$\begin{aligned} p_1(x) &= x^{\langle n \rangle} + \sum_{j=1}^{n-1} \delta_j x^{\langle j \rangle}, \\ p_2(x) &= x^{q^{n-1}} \Big(x^{\langle n-1 \rangle} + \sum_{j=1}^{n-1} \delta_j^{q^{-j}} x^{q^{n-j} \langle j-1 \rangle} \Big). \end{aligned} \tag{1}$$

Then $p_1(x^m)$ and $p_2(x^m)$ are isovalent for all $m \mid (q-1)$. Further, we have a factorization

$$p_1(x) - p_2(y) = G(x,y)(xG(x,y)^{q-1} - y^{q^{n-1}}), \tag{2}$$

where $G(x,y) \in F[x,y]$ is the polynomial of total degree $\langle n-1 \rangle$ given in equation (5). (*Also*, $\deg_x(G) = \deg_y(G) = \langle n-1 \rangle$.)

This theorem is essentially known to Fried; see [7, Section 5]. In particular, Fried anticipated the factorization of $p_1(x) - p_2(y)$ and calculated the degrees of the factors, and his proof shows that the isovalency condition

2000 *Mathematics Subject Classification*: 12E10, 12E05.

holds. Further insights can be found in Guralnick [9, Section 6]; in particular, the isovalency condition is carefully explained both at ramified and unramified points. The polynomial $p_1(x)$ is called a projective polynomial and has been studied by Abhyankar. The contribution of this article is that formulas for $p_2(y)$ and for the factorization of $p_1(x) - p_2(y)$ are given explicitly; also the methods of proof are new. The study of pairs (g, h) such that $g(x) - h(y)$ is reducible has a long history; see the articles of Cassels, Davenport, Lewis, Schinzel, Fried, Feit, Cassou-Noguès, and Couveignes in the bibliography. Our theorem provides examples of such factorizations.

The factors $G(x, y)$ and $H(x, y) := xG(x, y)^{q-1} - y^{q^{n-1}}$ of $p_1(x) - p_2(y)$ turn out to be absolutely irreducible in many examples. They satisfy a curious dependence: for any $a \in \overline{F}$, at least one of the polynomials $G(x, a)$ or $H(x, a)$ has a root in $K = F(a)$, because $p_1(x) - p_2(a)$ has a root in K. Similarly, $G(a, y)$ or $H(a, y)$ has a root in K.

Our proof of Theorem 1.1 is based on arithmetic properties of the roots of additive polynomials and their duals, which are derived in Section 2. For example, we prove that a separable additive or projective polynomial over a finite field F has the same number of rational roots as its dual. (This is false when the field F is infinite.)

Now we make some simple observations that apply generally to isovalent polynomials. We will say that two polynomials $g, h \in F[x]$ have the same *factorization type* if they have the same number of irreducible factors (counting repeated factors) of degree d for every $d \geq 1$. An equivalent condition is that g and h have the same number of roots in K (counting multiplicities) for every finite extension field K/F. Isovalent polynomials do not always have the same factorization type. The simplest example is the pair in $\mathbb{F}_2[x]$, $x^7 + x^3 + x = x(x^3 + x + 1)^2$ and $x^7 + x^6 + x^4 = x^4(x^3 + x^2 + 1)$. These are isovalent by Theorem 1.1, but their factorization types are different. Nonetheless, it is "usually" true that isovalent polynomials have the same factorization type, in the sense of the following lemma.

LEMMA 1.2. *Suppose g, h are isovalent. Then $g - a$ and $h - a$ have the same factorization type over $F(a)$ for all but finitely many $a \in \overline{F}$. Thus, g, h have the same degree.*

Proof. For $f \in F[x]$ define

$$S(f) = \{a \in \overline{F} \mid f - a \text{ has a multiple root}\} = \{f(b) \mid b \in \overline{F},\ f'(b) = 0\}.$$

$S = S(g) \cup S(h)$ is finite, since g' and h' have finitely many roots. Let $a \in \overline{F} - S$. Since g, h are isovalent, $g - a$ and $h - a$ have the same number of roots in L for all finite extensions $L/F(a)$, and since they are also multiplicity-free, they have the same factorization type. ∎

For the polynomials p_1, p_2 in the theorem, one can show that $p_1' = p_1/x$ and $p_2' = x^{\langle n\rangle - 1}$, so $S(p_1) = S(p_2) = \{0\}$. Thus, the fact that p_1 and p_2 are isovalent implies that $p_1 - a$ and $p_2 - a$ have the same factorization type over $F(a)$ for all nonzero $a \in \overline{F}$. When $a = 0$, then $p_1 - a$ and $p_2 - a$ have different factorization types, because (p_1, p_1') and (p_2, p_2') have different degrees. This phenomenon has an interesting interpretation in terms of monodromy groups. Let z be transcendental over F. By a result of Fried ([7, Section 5]), $p_1(x) - z$ and $p_2(x) - z$ have the same splitting field over $F(z)$, which we denote by Ω. Let T_1, T_2 denote the natural permutation representations of the monodromy group $G = \mathrm{Gal}(\Omega/F(z))$ acting on the roots of $p_1(x) - z$ and $p_2(x) - z$, respectively. Fried [6] showed that T_1 and T_2 are equivalent as representations, meaning that they have the same group characters. In particular, if $\sigma \in G$ then $T_1(\sigma^i)$ and $T_2(\sigma^i)$ have the same number of fixed points for all $i \geq 0$. Consequently, if H is a cyclic subgroup of G, then $T_1(H)$ and $T_2(H)$ have the same number of orbits of each size. One could ask whether the same is true for noncyclic subgroups of G. Apparently the answer is no. Consider the example $n = 3$, $F = \mathbb{F}_2$, $\delta_1 = \delta_2 = 1$, so $p_1 = x^7 + x^3 + x$, $p_2 = x^7 + x^6 + x^4$. Let H denote the inertia group at a place of Ω over $z = 0$. It turns out that the roots of $p_1(x) - z$ (resp. $p_2(x) - z$) can be put into bijection with the integers from 1 to 7 in such a way that

$$T_1(H) = \{1, (23)(67), (45)(67), (23)(45)\},$$
$$T_2(H) = \{1, (45)(67), (46)(57), (47)(56)\}.$$

Thus, $T_1(H)$ contains one fixed point and three orbits of size two, while $T_2(H)$ contains three fixed points and one orbit of size four. It would be interesting to compare the orbits of inertia groups for other isovalent pairs of polynomials. See Guralnick [9, Section 6] for further insights.

2. Adjoints of additive polynomials. This section contains new results about the relation between the roots of an additive or projective polynomial and the roots of its dual. These results are of independent interest, but also they are central to the proof that $p_1(x^m)$ and $p_2(x^m)$ are isovalent.

As before, let F be a finite field and q a power of $p = \mathrm{char}(F)$. Let $a_0, a_1, \ldots, a_n \in F$, $a_0 a_n \neq 0$. Define $f_1, f_2, \overline{f}_1, \overline{f}_2$ by the formulas

$$f_1(x) = \sum_{i=0}^{n} a_i x^{q^i}, \qquad f_2(x) = \sum_{i=0}^{n} (a_{n-i} x)^{q^i}, \qquad \overline{f}_i(x^{q-1}) = \frac{f_i(x)}{x}.$$

The polynomial $f_1(x)$ is called an $\mathbb{F}_q$-additive polynomial because it is $\mathbb{F}_q$-linear as a function on the algebraic closure $\overline{F}$. The polynomial f_2 is called the *adjoint* of f_1 and was studied by Oystein Ore [10] in the 1930's. The polynomials $\overline{f}_1$ and $\overline{f}_2$ are called *projective polynomials*, because their ge-

ometric monodromy groups are contained in the projective linear group $\mathrm{PGL}(n,q)$. Note that f_1, f_2 have no multiple roots, since their derivatives are nonzero constants. It follows easily that $\overline{f}_i(x^m)$ has no multiple roots, for any $m \mid (q-1)$.

We are indebted to John Dillon, who provided the proof of the following lemma in the case $c = 1$. The proof is perhaps more interesting than the lemma itself!

LEMMA 2.1. *Let $c \in \overline{F}$, and suppose $c^{q-1} \in F^\times$. Then the number of roots of f_1 in cF is equal to the number of roots of f_2 in $c^{-1}F$.*

Proof. Consider $\tau : \overline{F} \to \overline{F}$ defined by $\tau(x) = x^q$. Then $\tau : cF \to cF$, for if $\lambda \in F$ then $c^{-1}\tau(c\lambda) = c^{q-1}\lambda^q \in F$. Likewise $\tau : c^{-1}F \to c^{-1}F$. Define $T : cF \to cF$ by $T(x) = \sum a_i \tau^i(x)$, and define $S : F \to F$ by $S = c^{-1} \circ T \circ c$. Define $T^* : c^{-1}F \to c^{-1}F$ by $T^*(x) = \tau^{-n} \circ \sum (a_{n-i})^{q^i} \tau^i(x)$, and $S^* : F \to F$ by $S^* = c \circ T^* \circ c^{-1}$. All these maps are $\mathbb{F}_p$-linear, since τ is $\mathbb{F}_p$-linear. Consider the nondegenerate bilinear pairing on $F \times F$ given by $\langle x, y\rangle = \mathrm{Tr}(xy)$, where Tr denotes the absolute trace. For $(x,y) \in F \times F$ we have

$$\begin{aligned}\langle Sx, y\rangle &= \mathrm{Tr}(c^{-1}T(cx)y) = \mathrm{Tr}\Big(\sum a_i (cx)^{q^i} c^{-1} y\Big) \\ &= \mathrm{Tr} \sum \Big(a_i (cx)^{q^i} c^{-1} y\Big)^{q^{-i}} = \mathrm{Tr}\Big(\sum cx (a_i c^{-1} y)^{q^{-i}}\Big) \\ &= \mathrm{Tr}\Big(cx \sum (a_{n-i} c^{-1} y)^{q^{i-n}}\Big) = \mathrm{Tr}(xcT^*(c^{-1}y)) = \langle x, S^* y\rangle.\end{aligned}$$

This shows that S and S^* are adjoints of one another, hence have the same rank as endomorphisms of F over $\mathbb{F}_p$. Then $\mathrm{Ker}(S)$ and $\mathrm{Ker}(S^*)$ have the same dimension over $\mathbb{F}_p$. But $\mathrm{Ker}(S) = \{a \in F \mid f_1(ca) = 0\}$ and $\mathrm{Ker}(S^*) = \{a \in F \mid f_2(c^{-1}a) = 0\}$. Thus, the number of roots of f_1 in cF equals the number of roots of f_2 in $c^{-1}F$. ∎

THEOREM 2.2. *The additive polynomials f_1 and f_2 have the same factorization type. Also, $\overline{f}_1(x^m)$ and $\overline{f}_2(x^m)$ have the same factorization type whenever $m \mid (q-1)$.*

Proof. Let K be any finite extension field of F. By replacing F with K in Lemma 2.1, and setting $c = 1$, we see that f_1 and f_2 have the same number of roots in K, hence they have the same factorization type.

Let $ml = q - 1$, and set $h_1 = \overline{f}_1(x^m)$, $h_2 = \overline{f}_2(x^m)$; we will prove h_1, h_2 have the same factorization type. It suffices to prove they have the same number of roots in K, counting multiplicities. Since h_1 and h_2 have no multiple roots, it suffices to prove

$$|h_1^{-1}(0) \cap K| = |h_2^{-1}(0) \cap K|.$$

Suppose r_0 is a root of h_i, where $i \in \{1, 2\}$. Then $r_0 \neq 0$. There are l distinct

solutions in $\overline{F}$ to $r^l = r_0$, and for each such r, we have $f_i(r) = r\overline{f}_i(r^{ml}) = rh_i(r_0) = 0$. Clearly $r_0 \in K^\times$ if and only if $r \in K_l$, where

$$K_l = \{c \in \overline{F} \mid c^l \in K^\times\}.$$

Thus, there is an l-to-1 correspondence between roots of f_i which belong to K_l and roots of h_i which belong to K, i.e.,

$$|f_i^{-1}(0) \cap K_l| = l|h_i^{-1}(0) \cap K|, \quad i = 1, 2.$$

Let R be a complete set of coset representatives for $K_l/K^\times$. Then K_l is a disjoint union:

$$K_l = \bigcup_{c \in R} cK^\times = \bigcup_{c \in R} c^{-1}K^\times.$$

We have

$$\begin{aligned} l|h_1^{-1}(0) \cap K| &= |f_1^{-1}(0) \cap K_l| = \sum_{c \in R} |f_1^{-1}(0) \cap cK^\times| \\ &= \sum_{c \in R} |f_2^{-1}(0) \cap c^{-1}K^\times| \quad \text{by Lemma 2.1} \\ &= |f_2^{-1}(0) \cap K_l| = l|h_2^{-1}(0) \cap K|. \ \blacksquare \end{aligned}$$

We remark that Theorem 2.2 is false when f_1, f_2 are defined over an infinite field F. Bjorn Poonen supplied a counterexample over the rational function field $\mathbb{F}_3(a)$ with a transcendental: the function $f_1 = x^9 + ax^3 - (a+1)x$ vanishes at $x = 0, 1$, but $f_2 = x + a^3x^3 - (a+1)^9x^9$ has only one root ($x = 0$) in $\mathbb{F}_3(a)$. Nonetheless, it is true in general that f_1 and f_2 have the same splitting field; see Goss [8, Theorem 1.7.11]. We also remark that (for a general field F of finite characteristic) Elkies and Poonen independently found a nondegenerate, bilinear, Galois-invariant pairing between the vector space spanned by the roots of f_1 and the vector space spanned by the roots of f_2 (see [8, Definition 4.14.5]). There is a different proof of Lemma 2.1 using their pairing instead of the trace form.

3. Proof of Theorem 1.1

Proof that $p_1(x^m), p_2(x^m)$ are isovalent. Let K be a finite extension of F. For $a \in K$ and $f \in K[x]$, let $Z_K(f, a)$ denote the set of roots of $f(x) - a$ in K. We need to prove that if $m \mid (q-1)$, then

$$|Z_K(p_1(x^m), a)| = |Z_K(p_2(x^m), a)| \tag{3}$$

for all $a \in K$. In general, $|Z_K(f, 0)| = |K| - \sum_{a \in K^\times} |Z_K(f, a)|$. For this reason, it will suffice to show that (3) holds when $a \neq 0$. So, let $0 \neq a \in K$, and define $\overline{f}_1, \overline{f}_2 \in K[x]$ by

$$\overline{f}_1(x) = x^{\langle n\rangle} - a + \sum_{j=1}^{n-1} \delta_j x^{\langle j\rangle}, \qquad \overline{f}_2(x) = -ax^{\langle n\rangle} + 1 + \sum_{j=1}^{n-1} \delta_j^{q^{-j}} x^{\langle n-j\rangle}.$$

Then $x\overline{f}_2(x^{q-1})$ is the additive polynomial $-ax^{q^n} + x + \sum_{j=1}^{n-1} \delta_j^{q^{-j}} x^{q^{n-j}}$, and $x\overline{f}_1(x^{q-1})$ is the dual polynomial. Theorem 2.2 implies that $\overline{f}_1(x^m)$ and $\overline{f}_2(x^m)$ have the same number of roots in K counting multiplicities. Since all the roots of these polynomials are simple,

$$|Z_K(\overline{f}_1(x^m), 0)| = |Z_K(\overline{f}_2(x^m), 0)|.$$

Clearly $|Z_K(\overline{f}_1(x^m), 0)| = |Z_K(p_1(x^m), a)|$, since $\overline{f}_1 = p_1 - a$. Thus,

$$|Z_K(p_1(x^m), a)| = |Z_K(\overline{f}_2(x^m), 0)|.$$

To prove (3), we just need to show

$$|Z_K(\overline{f}_2(x^m), 0)| = |Z_K(p_2(x^m), a)|. \tag{4}$$

Let $\overline{f}_2^{\mathrm{rev}}(x) = x^{\langle n\rangle}\overline{f}_2(1/x)$, the reverse of $\overline{f}_2$. Since the roots of $\overline{f}_2$ are nonzero, $\overline{f}_2(x^m)$ has the same number of rational roots as $\overline{f}_2^{\mathrm{rev}}(x^m)$. A simple calculation using the identities $\langle n\rangle = q^{n-1} + \langle n-1\rangle$ and $q^{n-j}\langle j-1\rangle = \langle n-1\rangle - \langle n-j\rangle$ shows that $\overline{f}_2^{\mathrm{rev}}(x) = p_2(x) - a$, thus (4) holds as required.

Factorization of $p_1(x) - p_2(y)$. Define $R_i(y) \in F[y]$ for $0 \le i < n$ and $G(x,y) \in F[x,y]$ by

$$R_i(y) = y^{\langle i\rangle} + \sum_{j=1}^{i} \delta_{n-j}^{q^{j-n}} y^{q^j\langle i-j\rangle}, \qquad G(x,y) = \sum_{j=0}^{n-1} R_{n-1-j}(y)^{q^j} x^{\langle j\rangle}. \tag{5}$$

Note that $R_0 = 1$ and $R_i(y) = y^{q^{i-1}} R_{i-1}(y) + \delta_{n-i}^{q^{i-n}}$ when $1 \le i \le n-1$. We have

$$\begin{aligned}
xG(x,y)^q &= \sum_{j=0}^{n-1} R_{n-1-j}(y)^{q^{j+1}} x^{\langle j+1\rangle} = x^{\langle n\rangle} + \sum_{j=1}^{n-1} R_{n-j}(y)^{q^j} x^{\langle j\rangle} \\
&= x^{\langle n\rangle} + \sum_{j=1}^{n-1} (y^{q^{n-j-1}} R_{n-j-1} + \delta_j^{q^{-j}})^{q^j} x^{\langle j\rangle} \\
&= y^{q^{n-1}} \sum_{j=1}^{n-1} R_{n-j-1}(y)^{q^j} x^{\langle j\rangle} + p_1(x) \\
&= y^{q^{n-1}} (G(x,y) - R_{n-1}(y)) + p_1(x) \\
&= y^{q^{n-1}} G(x,y) - p_2(y) + p_1(x). \ \blacksquare
\end{aligned}$$

Acknowledgements. The author would like to thank John Dillon for his elegant proof that an additive polynomial and its adjoint have the same

factorization type. She also thanks Michael Zieve for some stimulating questions that led to a much stronger Theorem 1.1. Originally the author considered only the "additive" case $m = q-1$; Zieve encouraged her to look at the "projective" case $m = 1$. In addition, Zieve asked whether $p_1(x) - p_2(y)$ was reducible, and he pointed out that one of the author's hypotheses ($\mathbb{F}_q \subset F$) was unnecessary.

References

[1] J. W. S. Cassels, *Factorization of polynomials in several variables*, in: Proc. 15th Scandinavian Congress (Olso, 1968), Lecture Notes in Math. 118, Springer, 1970, 1–17.

[2] P. Cassou-Noguès et J.-M. Couveignes, *Factorisations explicites de $g(y)-h(z)$*, Acta Arith. 87 (1999), 291–317.

[3] H. Davenport, D. J. Lewis, and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312.

[4] H. Davenport and A. Schinzel, *Two problems concerning polynomials*, J. Reine Angew. Math. 214 (1964), 386–391. Corrigendum, ibid. 218 (1965), 220.

[5] W. Feit, *Automorphisms of balanced incomplete block designs*, Math. Z. 118 (1970), 40–49.

[6] M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. 17 (1973), 128–146.

[7] —, *Variables separated polynomials, the genus* 0 *problem and moduli spaces*, in: Number Theory in Progress (Zakopane-Kościelisko, 1997), Vol. 1, Walter de Gruyter, 1999, 169–228.

[8] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergeb. Math. Grenzgeb. (3) 35, Springer, 1996.

[9] R. M. Guralnick, *Rational maps and images of rational points of curves over finite fields*, Irish Math. Soc. Bull. 50 (2003), 71–95.

[10] O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. 35 (1933), 559–584.

[11] A. Schinzel, *Some unsolved problems on polynomials*, in: Neki nerešeni problemi u matematici [Some Unsolved Problems in Mathematics], Matematička Biblioteka 25, Zavod za Izdavanje Udžbenika, Belgrade, 1963, 63–70.

Mathematics Research Group
National Security Agency
9800 Savage Road, Suite 6515
Fort George G. Meade, MD 20755-6515, U.S.A.
E-mail: bluher@afterlife.ncsc.mil

Received on 16.4.2003
and in revised form on 29.9.2003 (4511)