2004

Pencils of Quadratic Forms over Finite Fields

Robert W. Fitzgerald
Southern Illinois University Carbondale, rfitzg@math.siu.edu

Joseph L. Yucas
Southern Illinois University Carbondale

Published in *Discrete Mathematics*, 283, 71-79.

Pencils of Quadratic Forms over Finite Fields

Robert W. Fitzgerald and Joseph L. Yucas

Abstract

A formula for the number of common zeros of a non-degenerate pencil of quadratic forms is given. This is applied to pencils which count binary strings with an even number of 1's prescribed distances apart.

1 Introduction

Let p be a prime and let q be a power of p. F will denote the finite field of order q and characteristic p.

A *quadratic form* of *dimension* d over F is a pair (V, Q), where V is a d-dimensional vector space over F and $Q : V \to F$ is a mapping satisfying:

(i) $Q(ax) = a^2Q(x)$ for all $a \in F$ and $x \in V$ and
(ii) The mapping $B_Q : V \times V \to F$ defined by

$$B_Q(x, y) = Q(x + y) - Q(x) - Q(y)$$

is symmetric and bilinear.

We say that a quadratic form Q on V is *degenerate* if there is some non-zero $x \in V$ such that $B_Q(x, y) = 0$ for all $y \in V$. Q is *non-degenerate* otherwise.

Suppose Q_1 and Q_2 are quadratic forms defined on V. The *sum* of Q_1 and Q_2 is the quadratic form Q on V defined by, $Q(x) = Q_1(x) + Q_2(x)$. If $a \in F$ and Q is a quadratic form on V then aQ defined by, $(aQ)(x) = aQ(x)$, is a quadratic form on V. The collection of all quadratic forms on V is a vector space over F and will be denoted by $Q(V)$.

A subspace of $Q(V)$ is called a *pencil* on V. A pencil is said to be *non-degenerate* if every non-zero quadratic form in the pencil is non-degenerate.

In Section 2, we generalize a counting technique that we used in [3]. Theorem 2 gives a formula for the number of common zeros of a non-degenerate pencil in terms of the discriminants or Arf invariants of the forms in the pencil.

Motivated by their combinatorial application we study, in Section 3, pencils that are spanned by gap forms (see Section 3 for the definition of gap form). For these pencils we can finesse the computations of the invariants. This is done in Section 4. This gives rise to a formula for the number of common zeros of a non-degenerate pencil spanned by gap forms.

Finally, in Section 5, we give the combinatorial implications of these results.

2 Quadratic forms

If the characteristic, p, of F is odd then every non-degenerate quadratic form Q on V can be diagonalized, that is, is isometric to a quadratic form on F^d of the type $a_1x_1^2 + a_2x_2^2 + \ldots + a_dx_d^2$ for some $a_i \in F$. The *discriminant* of Q is $(-1)^{d(d-1)/2}\prod_{i=1}^{d} a_i \in \dot{F}/\dot{F}^2$. If p is even then $d = 2e$ is even and V possesses a symplectic basis $\{u_1, v_1, \ldots, u_e, v_e\}$. The *Arf invariant* of Q is $\sum_{i=1}^{e} Q(u_i)Q(v_i) \in F/PF$ where $PF = \{a + a^2 : a \in F\}$.

For a quadratic form Q on V we define Λ by

$$\Lambda(Q) = \begin{cases} \text{discriminant of } Q & \text{if } p \text{ is odd} \\ \text{Arf invariant of } Q & \text{if } p \text{ is even} \end{cases}.$$

$\Lambda(Q)$ will be called simply, the *invariant* of Q.

For $a \in F$, we use $N(Q = a)$, to denote the number of solutions to $Q(x) = a$. The following Theorem is implicit in Theorem 6.26 and Theorem 6.32 of [5].

Theorem 1 *Let Q be a non-degenerate quadratic form of dimension $d = 2e$ over F.*

$$N(Q = 0) = \begin{cases} q^{2e-1} + q^e - q^{e-1} & \textit{if } \Lambda(Q) \textit{ is trivial} \\ q^{2e-1} - q^e + q^{e-1} & \textit{otherwise} \end{cases}.$$

If $\mathbf{P}$ is a pencil on V and $a \in F$, N($\mathbf{P}$ = a) will denote the number of solutions to the system $\{Q(x) = a : Q \in \mathbf{P}\}$.

Theorem 2 *Let V be a $d = 2e$-dimensional vector space over F and suppose* $\mathbf{P}$ *is an r-dimensional non-degenerate pencil on V with $r \le e$. Then*

$$N(\mathbf{P}=0) = 2\mathrm{q}^{\mathrm{e-r}}\lambda + \mathrm{q}^{\mathrm{2e-r}} - \mathrm{q}^{\mathrm{e}} + \mathrm{q}^{\mathrm{e-r}}$$

where λ is the number of non-zero quadratic forms in $\mathbf{P}$ *with trivial invariant.*

Proof: Let $\{Q_1, Q_2, \ldots, Q_r\}$ be a basis for $\mathbf{P}$. For $v = (v_1, v_2, \ldots, v_r) \in F^r$, let $Q_v = \sum_{i=1}^r v_i Q_i$. For $x \in V$, $Q_v(x) = \sum_{i=1}^r v_i Q_i(x) = v \cdot w(x)$, where $w(x) = (Q_1(x), Q_2(x), \ldots, Q_r(x))$. For fixed $w \in F^r$, let $N(w)$ be the number of $x \in V$ with $w(x) = w$. We have,

$$\sum_{w \in F^r, w\cdot v=0} N(w) = N(Q_v = 0) \qquad (1)$$

We will now sum (1) over all non-zero $v \in F^r$. Notice that for each $v \in F^r$, $N(0)$ occurs as a summand of the left hand side of (1). Also, if w is non-zero, there are $q^{r-1} - 1$ non-zero $v \in F^r$ with $w \cdot v = 0$. By Theorem 1, the right hand side of (1) is $A = q^{2e-1} + q^e - q^{e-1}$ if $\Lambda(Q_v)$ is trivial or $B = q^{2e-1} - q^e + q^{e-1}$ if $\Lambda(Q_v)$ is non-trivial. Summing (1) over all non-zero $v \in F^r$ yields

$$(q^r - 1)N(0) + (q^{r-1} - 1) \sum_{0 \ne w \in F^r} N(w) = \lambda A + (q^r - 1 - \lambda)B.$$

Now,

$$\sum_{0 \ne w \in F^r} N(w) = \sum_{w \in F^r} N(w) - N(0) = q^{2e} - N(0)$$

hence

$$\begin{aligned}(q^r - q^{r-1})N(0) &= \lambda A + (q^r - 1 - \lambda)B - (q^{r-1} - 1)q^{2e} \\ &= \lambda(A - B) + (q^r - 1)B - (q^{r-1} - 1)q^{2e}.\end{aligned}$$

Notice that $A - B = 2(q^e - q^{e-1})$ and

$$(q^r - 1)B - (q^{r-1} - 1)q^{2e} = (q - 1)(-q^{r+e-1} + q^{2e-1} + q^{e-1}).$$

Consequently,

$$q^{r-1}(q - 1)N(0) = 2\lambda q^{e-1}(q - 1) + (q - 1)(-q^{r+e-1} + q^{2e-1} + q^{e-1})$$

and

$$N(0) = 2q^{e-r}\lambda + q^{2e-r} - q^e + q^{e-r}.$$

Finally, note that $N(\mathbf{P} = 0) = \mathrm{N}(0)$.

■

If char(F) is even then any odd dimensional form is degenerate. However, when char(F) is odd we get a simplified version of Theorem 2, which does not depend on invariants.

Theorem 3 *Suppose char(F) is odd and let V be a d-dimensional space over F with d odd.*

(1) If Q is a non-degenerate quadratic form over V then

$$N(Q = 0) = q^{d-1}.$$

(2) Let $\mathbf{P}$ be an r-dimensional non-degenerate pencil on V with $r \leq d-1$. Then:

$$N(\mathbf{P} = 0) = \mathrm{q}^{\mathrm{d-r}}.$$

Proof: The proof of (1) follows from [5]. The proof of (2) is the same as the proof of Theorem 2 but with (1) replacing Theorem 1.

■

3 Gap forms

Throughout this section we continue to assume that F is the finite field of order q and characteristic p. Let K be a finite extension of F of odd degree $n = 2m + 1$. Recall that the trace map from K onto F is defined by

$$tr(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}}.$$

For each $1 \leq i \leq n-1$, we consider the *i-th gap form* defined for $\alpha \in K$ by:

$$Q_i(\alpha) = tr(\alpha\alpha^{q^i}).$$

Notice that $Q_{n-i} = Q_i$ for each $i = 1, 2, \ldots, n-1$. Consequently, we need only consider Q_i for $i = 1, 2, \ldots, m$.

These forms have been studied before. They appear in [1] where a result of Welch (Theorem 16.46) gives the number of zeros of Q_k when k divides n. In this case Q_k is degenerate whereas we only consider non-degenerate forms. Berlekamp uses Welch's result to find weight enumerators of double-error correcting binary BCH codes. Scaled versions of gap forms also appeared in [2] where they were also used to compute certain weight enumerators. Our interest will be in counting binary strings with prescribed gaps.

Proposition 4 *The i-th gap form, Q_i, has associated symmetric form $B_i : K \times K \to F$ given by:*

$$B_i(\alpha, \beta) = tr(\alpha\beta^{q^i} + \beta\alpha^{q^i}) = tr((\alpha^{q^i} + \alpha^{q^{n-i}})\beta).$$

In particular, B_i is bilinear and Q_i is a quadratic form on K.

Proof: : $Q_i(\alpha+\beta) - Q_i(\alpha) - Q_i(\beta) = tr((\alpha+\beta)(\alpha+\beta)^{q^i}) - tr(\alpha\alpha^{q^i}) - tr(\beta\beta^{q^i}) = tr(\alpha\beta^{q^i} + \beta\alpha^{q^i}) = tr((\alpha^{q^i} + \alpha^{q^{n-i}})\beta)$ since $tr(\alpha\beta^{q^i}) = tr(\alpha^{q^{n-i}}\beta)$. It is easy to see that B_i is bilinear. For $a \in F$, notice that $Q_i(a\alpha) = tr((a\alpha)(a\alpha)^{q^i}) = tr(aa^{q^i}\alpha\alpha^{q^i}) = a^2Q_i(\alpha)$. Hence Q_i is a quadratic form on K.

■

In the notation of Theorem 2.24 of [5], $B_i(\alpha, \beta) = L_{\alpha^{q^i}+\alpha^{q^{n-i}}}(\beta)$.

Notice that if char(F) is even then for each $1 \leq i \leq n-1$, Q_i is degenerate since $B_i(1, \beta) = 0$ for all $\beta \in K$. However when char(F) is odd, these forms are non-degenerate. The proof follows.

Lemma 5 *Suppose char(F) is odd and $k \geq 1$. Every irreducible factor of $x^{q^k-1} + 1$ has even degree.*

Proof: Let $f(x)$ be an irreducible factor of $x^{q^k-1} + 1$ and suppose α is a root of $f(x)$ in the splitting field of $f(x)$. Since $-\alpha = \alpha^{q^k}$, we see that $-\alpha$ is also a root of $f(x)$. Now, $\alpha \neq -\alpha$ since char(F) is odd. Consequently, $f(x)$ has a factorization of the form $\prod(x^2 - \alpha_i^2)$ in its splitting field.

■

Proposition 6 *For $1 \leq i \leq m$, Q_i is non-degenerate on K when char(F) is odd.*

Proof: Suppose α is a non-zero element of K and $B_i(\alpha, \beta) = 0$ for all $\beta \in K$. By Proposition 4, $L_{\alpha^{q^i}+\alpha^{q^{n-i}}} = 0$ and hence by Theorem 2.24 of [5], $\alpha^{q^i} + \alpha^{q^{n-i}} = 0$. Raising each side to the $(q^i)^{th}$ power yields $\alpha^{q^{2i}} + \alpha = 0$ and thus α satisfies $x^{q^k-1} + 1$. By Lemma 5, $[F(\alpha) : F]$ is even. But $[F(\alpha) : F]$ divides n and n is odd, a contradiction.

■

Set $K_0 = ker(tr)$. We will study the restriction of Q_i to K_0.

Lemma 7 *Suppose char(F) does not divide n. If $\gamma \in K_0$ and $L_\gamma(\beta) = 0$ for all $\beta \in K_0$ then $\gamma = 0$.*

Proof: $ker(L_\gamma) = K$ or $ker(L_\gamma) = K_0$. Hence $L_\gamma = L_a$ for some $a \in F$. By Theorem 2.24 of [5], $\gamma = a$. Now $\gamma \in K_0$, hence $0 = tr(a) = na$. Since char(F) does not divide n, we see that $a = \gamma = 0$.

■

Lemma 8 *Suppose char(F) does not divide n. For $1 \leq i_1 < i_2 < \ldots < i_r \leq m$, let $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ be gap forms on K_0 and let $Q = a_{i_1}Q_{i_1} + a_{i_2}Q_{i_2} + \ldots + a_{i_r}Q_{i_r}$ for some $a_{i_j} \in F$. If Q is degenerate on K_0 then there is a nonzero $\alpha \in K_0$ satisfying the polynomial*

$$p(x) = \sum_{j=1}^{r}(a_{i_j}x^{q^{i_r+i_j}} + a_{i_j}x^{q^{i_r-i_j}}).$$

Proof: By Proposition 4, the associated bilinear symmetric form for Q is given by $B_Q(\alpha, \beta) = L_\gamma(\beta)$, where $\gamma = \sum_{j=1}^{r} a_{i_j}\alpha^{q^{i_j}} + a_{i_j}\alpha^{q^{n-i_j}}$. If Q is degenerate then there is a nonzero $\alpha \in K_0$ with $L_\gamma(\beta) = 0$ for all $\beta \in K_0$. Notice that $\gamma \in K_0$ since α is. By Lemma 7, $\gamma = 0$. Consequently, $\gamma^{q^{i_r}} = \sum_{j=1}^{r} a_{i_j}\alpha^{q^{i_r-i_j}} + a_{i_j}\alpha^{q^{i_r+i_j}} = 0$.

■

We will use the notation (a, b) to denote the greatest common divisor of a and b.

Proposition 9 *For $1 \leq i \leq m$,*

1. If char(F) is odd then Q_i is non-degenerate on K_0 if and only if char(F) does not divide n.

2. If char(F) is even with $(n, i) = 1$ then Q_i is non-degenerate on K_0.

Proof: 1. Assume char(F) does not divide n and suppose $\alpha \in K_0$ with $B_i(\alpha, \beta) = 0$ for all $\beta \in K_0$. We show that Q_i is degenerate on K contradicting Proposition 6. Let $\gamma \in K$. Set $g = \frac{tr(\gamma)}{n}$ and let $\gamma_0 = \gamma - g$. Since $g \in F$, $tr(\gamma_0) = tr(\gamma) - ng = 0$ hence $\gamma_0 \in K_0$. Now, since $B_i(\alpha, \gamma_0) = 0$ we have

$$B_i(\alpha, \gamma) = B_i(\alpha, g) = tr(\alpha^{q^i}g + \alpha g^{q^i})$$

$$= tr(\alpha^{q^i}g + \alpha g) = (g)tr(\alpha^{q^i} + \alpha) = (2g)tr(\alpha) = 0$$

since $\alpha \in K_0$. Consequently, Q_i is degenerate on K. Conversely, if char(F) divides n then $tr(1) = n = 0$ and $1 \in K_0$. For any $\beta \in K_0$, we have $B_i(1,\beta) = tr(\beta + \beta^{q^i}) = 2tr(\beta) = 0$. Hence, Q_i is degenerate on K_0.

2. If Q_i is degenerate on K_0 then by Lemma 8, there is a nonzero $\alpha \in K_0$ with $\alpha^{q^{2i}} = \alpha$. Suppose that $F(\alpha) = GF(q^s)$. We then have, s divides $2i$ and s divides n. But n is odd and $(n,i) = 1$, thus $s = 1$ and $\alpha \in F$. Recall that $tr(\alpha) = 0$ but since n is odd, $tr(1) = 1$. Hence $\alpha = 0$, a contradiction.

∎

A polynomial of the form

$$L(x) = \sum_{j=1}^{s} a_j x^{2^j}$$

with $a_j \in F$ is called a *linearized* polynomial over F. The polynomial

$$l(x) = \sum_{j=1}^{s} a_j x^j$$

will be called the *nonlinearization* of $L(x)$. The following result follows from Theorem 3.6.3 of [5].

Proposition 10 *Let $L(x)$ be a linearized polynomial over F and let $l(x)$ be its nonlinearization. If $f(x)$ is an irreducible factor of $L(x)$ of degree d then d divides the order of $l(x)$.*

Corollary 11 *Suppose char(F) does not divide n. For $1 \le i_1 < i_2 < \ldots i_r \le m$, there is a positive integer π^* such that if $(n,\pi^*) = 1$ the pencil spanned by $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ is non-degenerate on K_0.*

Proof: Let $Q_{j_1}, Q_{j_2}, \ldots, Q_{j_t}$ be a subset of $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ and let $Q = a_{j_1}Q_{j_1} + a_{j_2}Q_{j_2} + \ldots + a_{j_t}Q_{j_t}$ for some $a_{j_i} \in F$. If Q is degenerate, then by Lemma 8, there is some nonzero $\alpha \in K_0$ satisfying

$$L(x) = \sum_{k=1}^{t} (a_{j_k} x^{q^{j_t} - q^{j_k}} + a_{j_k} x^{2^{j_t} + 2^{j_k}}).$$

Let d be the degree of the irreducible polynomial of α over F. Since $\alpha \notin F$, we see that $d > 1$. Also, $[F(\alpha) : F] = d$, so d divides n. Let π be the order of the nonlinearization $l(x)$ of $L(x)$. By Proposition 10, d divides π.

If $(n, \pi) = 1$, we get a contradiction. Repeat this argument for every linear combination of every subset of $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ and let π^* be the product of all distinct primes dividing a resulting π.

■

Example: Suppose $q = 2$ and $\mathbf{P}$ is spanned by Q_1, Q_2, Q_3, Q_4, Q_5. Then the π^* of Corollary 11 is $3 \cdot 5 \cdot 7 \cdot 17$. This is computed as in the above proof, by finding the orders of the appropriate nonlinearizations.

■

4 The invariants

In this section we continue to assume that F is the finite field of order q and characteristic p. K however will be a finite extension of F of odd prime degree $n = 2m + 1$. In this case we then can compute the invariants of gap forms in non-degenerate pencils.

Lemma 12 *Suppose $n = 2m + 1$ is prime, $n \neq char(F)$, and r is a positive integer. Let $(\frac{q}{n})$ denote the Legendre symbol. The congruence*

$$2q^{m-r}s + q^{2m-r} - q^m + q^{m-r} \equiv 1 \ (mod\ n)$$

has solution

$$s = \begin{cases} q^r - 1 \ (mod\ n) & if\ (\frac{q}{n}) = 1 \\ 0 \ (mod\ n) & if\ (\frac{q}{n}) = -1 \end{cases} .$$

Proof: Let $\epsilon = (\frac{q}{n})$. By Euler's Criterion, $q^m \equiv \epsilon$ (mod n). Multiplying the above congruence by q^r yields

$$2q^m s + q^{2m} - q^{m+r} + q^m \equiv q^r \text{ (mod n)}$$

$$2\epsilon s + 1 - q^r \epsilon + \epsilon \equiv q^r \text{ (mod n)}$$

$$2\epsilon s \equiv (q^r - 1)(\epsilon + 1) \text{ (mod n)}.$$

If $\epsilon = 1$ then $s \equiv q^r - 1$ (mod n). If $\epsilon = -1$ then $s \equiv 0$ (mod n).

■

Theorem 13 *Let $n = 2m + 1$ be prime. For $1 \leq i_1 < i_2 < \ldots < i_r \leq m$, suppose that $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ are gap forms on K_0 that span a non-degenerate pencil* $\mathbf{P}$. *If $n \neq char(F)$ and $n \geq (q-1)^r$ then the number, λ, of non-zero quadratic forms in* $\mathbf{P}$ *that have trivial invariant is given by*

$$\lambda = \begin{cases} q^r - 1 & \text{if } (\frac{q}{n}) = 1 \\ 0 & \text{if } (\frac{q}{n}) = -1 \end{cases} .$$

Proof: First notice that if $\alpha \in K_0$ is non-zero then $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ are distinct since n is prime. Further, $Q_i(\alpha^{q^j}) = tr(\alpha^{q^j}\alpha^{q^{i+j}}) = tr((\alpha\alpha^{q^i})^{q^j}) = tr(\alpha\alpha^{q^i}) = Q_i(\alpha)$. Consequently, $N(\mathbf{P} = 0) - 1$, the number of common non-zero solutions for the quadratic forms in $\mathbf{P}$, will be divisible by n. By Theorem 2, we have

$$2q^{m-r}\lambda + q^{2m-r} - q^m + q^{m-r} \equiv 1 \text{ (mod n)}$$

We prove the Theorem by induction on r. If $r = 1$, the result follows from Lemma 12. By induction, each (r-1)-subset of $\{Q_{i_1}, Q_{i_2}, ..., Q_{i_r}\}$ spans a pencil containing $q^{r-1} - 1$ non-zero quadratic forms with trivial invariant if $(\frac{q}{n}) = 1$ or containing no non-zero quadratic forms with trivial invariant if $(\frac{q}{n}) = -1$. The non-zero forms of $\mathbf{P}$ not considered yet have the form $a_{i_1}Q_{i_1} + a_{i_2}Q_{i_2} + \ldots + a_{i_r}Q_{i_r}$ with $a_{i_j} \neq 0$ for each j. There are $(q-1)^r$ of these. Suppose t of these have trivial invariant. In the case when $(\frac{q}{n}) = 1$ we then have $\lambda = (q^r - 1) - (q-1)^r + t$. By Lemma 12, $\lambda \equiv q^r - 1 \pmod{n}$. So $t \equiv (q-1)^r \pmod{n}$. By assumption, $n > (q-1)^r \geq t$. Thus $t = (q-1)^r$ and $\lambda = q^r - 1$. In the case when $(\frac{q}{n}) = -1$ we have, $\lambda = t$. By Lemma 12 again, $t \equiv 0 \pmod{n}$. Again $n > t \geq 0$ implies $t = 0$ and so $\lambda = 0$.

■

Note that when $q = 2$, the conditions that $n \neq \text{char}(F)$ and $n > (q-1)^r$ always hold for odd primes n.

We pause to make two further remarks. First notice that it was a special property of gap forms that allowed us to finesse the computation of the invariants in Theorem 13. Namely, $Q_i(\alpha) = Q_i(\alpha^{q^j})$. In general, the invariants are usually computed by their definitions. Secondly, Theorem 13 is not true for arbitrary non-degenerate pencils. We illustrate these remarks in the following example.

Example: Let $F = GF(2)$ and $V = F^4$. Consider the quadratic forms defined for $x = (x_1, x_2, x_3, x_4) \in V$ by $q_1(x) = x_1x_3 + x_2x_4, q_2(x) = x_1^2 + x_1x_3 + x_1x_4 + x_2x_3 + x_3^2$ and $q(x) = q_1(x) + q_2(x) = x_1^2 + x_2x_4 + x_2x_3 +$

$x_2x_4 + x_3^2$. Their associated symmetric bilinear forms are $b_1(x,y) = x_1y_3 + x_2y_4 + x_3y_1 + x_4y_2, b_2(x,y) = x_1y_3 + x_3y_1 + x_1y_4 + x_4y_1 + x_2y_3 + x_3y_2$ and $b_q(x,y) = x_1y_4 + x_4y_1 + x_2y_3 + x_3y_2 + x_2y_4 + x_4y_2$ respectively. They are easily seen to be non-degenerate. Respective symplectic bases are

$$\{u_1 = (1,0,1,0), v_1 = (1,0,0,0), u_2 = (0,0,0,1), v_2 = (0,1,0,0)\}$$

$$\{u_1 = (1,0,0,0), v_1 = (0,0,1,0), u_2 = (1,1,0,0), v_2 = (0,0,1,1)\},$$

and

$$\{u_1 = (1,0,0,0), v_1 = (0,0,0,1), u_2 = (0,0,1,0), v_2 = (1,1,0,0)\}.$$

Using $\Lambda(Q) = \sum Q(u_i)Q(v_i)$, we see that $\Lambda(q_1) = 0, \Lambda(q_2) = 0$ and $\Lambda(q) = 1$.

■

Corollary 14 *Let $n = 2m+1$ be prime. For $1 \leq i_1 < i_2 < \ldots < i_r \leq m$, suppose that $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ are gap forms on K_0 that span a non-degenerate pencil $\mathbf{P}$. If $n \neq char(F)$ and $n \geq (q-1)^r$ then the number, $N(\mathbf{P} = 0)$, is given by*

$$N(\mathbf{P} = 0) = \begin{cases} q^{m-r}(q^m + q^r - 1) & \text{if } (\frac{q}{n}) = 1 \\ q^{m-r}(q^m - q^r + 1) & \text{if } (\frac{q}{n}) = -1 \end{cases}.$$

Proof: This follows from Theorem 2 and Theorem 13.

■

5 Application

In this section we restrict our attention to the case $F = GF(2)$, and $K = GF(2^n)$. We continue to assume that $n = 2m+1$ is an odd positive integer. A normal basis $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ for K over F is *self-dual* if $tr(\alpha^{2^i}\alpha^{2^j}) = \delta_{ij}$. See Theorem 5.2.1 of [4] for the existence of such a basis.

There is an interesting combinatorial perspective of the gap forms. Let $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ be a self-dual normal basis for K over F and let $\gamma = c_0\alpha + c_1\alpha^2 + \ldots + c_{n-1}\alpha^{2^{n-1}} \in K$. Since $tr(\alpha^{2^i}) = 1$, for $0 \leq i \leq n-1$, we see that $tr(\gamma) = c_0 + c_1 + \ldots + c_{n-1} \pmod 2$. Hence $\gamma \in K_0$ means that the string $(c_0, c_1, \ldots, c_{n-1})$ has even weight. $Q_i(\gamma) = tr(\gamma\gamma^{2^i}) = tr((c_0\alpha + c_1\alpha^2 +$

$\ldots + c_{n-1}\alpha^{2^{n-1}})(c_0\alpha^{2^i} + c_1\alpha^{2^{i+1}} + \ldots + c_{n-1}\alpha^{2^{i-1}}))$. Since $tr(\alpha^{2^j}\alpha^{2^k}) = \delta_{jk}$, we see that $Q_i(\gamma) = c_0c_i + c_1c_{i+1} + \ldots + c_{n-i-1}c_{n-1} + c_{n-i}c_0 + \ldots + c_{n-1}c_{i-1} \pmod 2$. Consequently, $Q_i(\gamma) = 0$ means that the string $(c_0, c_1, \ldots, c_{n-1})$ has an even number of pairs of 1's which are a distance of i coordinates apart.

Before our study of these strings we first record a few results on pencils spanned by gap forms over $GF(2)$.

Proposition 15 *For $1 \le i_1 < i_2 \le m$ with $(n, i_1) = (n, i_2) = (n, i_2 \pm i_1) = 1$, the pencil $\mathbf{P}$ spanned by Q_{i_1} and Q_{i_2} is non-degenerate on K_0.*

Proof: By Proposition 9(2), it suffices to show that $Q = Q_i + Q_j$ is non-degenerate on K_0. If Q is degenerate on K_0 then by Lemma 8, there is a nonzero $\alpha \in K_0$ with $\alpha^{2^{i_2+i_1}} + \alpha^{2^{i_2-i_1}} + \alpha^{2^{2i_2}} + \alpha = 0$. Let $\eta = \alpha + \alpha^{2^{i_2-i_1}}$. Then $\eta + \eta^{2^{i_2+i_1}} = 0$. Let $F(\eta) = GF(2^s)$. Then s divides $i_2 + i_1$ and s divides n. Since $(n, i_2 + i_1) = 1$ we have $s = 1$ and $\eta \in F$. Since $tr(\eta) = 0$, we see that $\eta = 0$. Consequently, $\alpha^{2^{i_2-i_1}} = \alpha$. Let $F(\alpha) = GF(2^t)$. Then t divides $i_2 - i_1$ and t divides n. Since $(n, i_2 - i_1) = 1$ we have $t = 1$ and $\alpha \in F$. Since $tr(\alpha) = 0$, we have $\alpha = 0$, a contradiction.

■

We remark that Proposition 15 also holds for $q = 3$. One needs only check that $Q_{i_1} + Q_{i_2}$ and $Q_{i_1} - Q_{i_2}$ are both non-degenerate. The proofs are essentially the same as the one given above for $Q_{i_1} + Q_{i_2}$. For $q > 3$ however, Proposition 15 fails. $3Q_1 + Q_2$ is degenerate for $n = 13$ over $GF(5)$.

Proposition 16 *For $1 \le i_1 < i_2 < i_3 \le m$ suppose $(n, i_1) = (n, i_2) = (n, i_3) = (n, i_2 \pm i_1) = (n, i_3 \pm i_1) = (n, i_3 \pm i_2) = 1$. If $i_3 - i_2 = i_2 - i_1$, then the pencil $\mathbf{P}$ spanned by Q_{i_1}, Q_{i_2} and Q_{i_3} is non-degenerate on K_0.*

Proof: By Proposition 15, it suffices to show that $Q = Q_{i_1} + Q_{i_2} + Q_{i_3}$ is non-degenerate on K_0. If Q is degenerate on K_0 then by Lemma 8, there is a nonzero $\alpha \in K_0$ with $\alpha^{2^{i_3+i_1}} + \alpha^{2^{i_3-i_1}} + \alpha^{2^{i_3+i_2}} + \alpha^{2^{i_3-i_2}} + \alpha^{2^{2i_3}} + \alpha = 0$. Let $\eta = \alpha + \alpha^{2^{i_3+i_1}}$. Since $i_3 - i_2 = i_2 - i_1$ we see that η satisfies

$$L(x) = x + x^{2^{i_2-i_1}} + x^{2^{2(i_2-i_1)}}.$$

Let d be the degree of the irreducible polynomial of η over F. By Proposition 10, d divides the order of $l(x) = x^{2(i_2-i_1)} + x^{i_2-i_1} + 1$. Since $x^{3(i_2-i_1)} + 1 = l(x)(x^{i_2-i_1} + 1)$, we see that d divides $3(i_2 - i_1)$. We also know that d divides n. Now, at least two of $i_3 \pm i_1, i_2 \pm i_1$ are the same mod 3, hence 3 divides one of $i_3, i_2, i_3 + i_2$ or $i_3 - i_2$. Consequently, by our hypothesis, 3 does not divide n. We have d dividing $i_2 - i_1$ and d dividing n. Since $(n, i_2 - i_1) = 1$, we see that $d = 1$ and $\eta = 0$. Let $F(\alpha) = GF(2^t)$. Then t divides $i_3 + i_1$ and t divides n. Since $(n, i_3 + i_1) = 1$ we have $t = 1$ and $\alpha \in F$, a contradiction.

■

We remark that the conclusions of Proposition 9(2), Proposition 15, and Proposition 16 are not true in general. Q_3 and $Q_1 + Q_2$ are degenerate when $n = 9$ and $Q_2 + Q_4 + Q_5$ is degenerate when $n = 17$ over $GF(2)$.

Proposition 17 *Suppose $n = 2m + 1$ is prime and suppose $1 \le i_1 < i_2 < \ldots < i_r \le m$. If $n > 2^{2i_r - 1} - 1$ then the pencil spanned by $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_r}$ is non-degenerate on K_0.*

Proof: The nonlinearization polynomials considered in the proof of Corollary 11 have the form $\sum_{j=1}^{t}(x^{t+j} + x^{t-j})$. In particular, their orders are less than or equal to $2^{2i_r} - 1$. Since $x + 1$ is a factor of each of these characteristic polynomials, their orders are even. Consequently, any odd prime dividing one of these orders will be less than or equal to $2^{2i_r - 1} - 1$.

■

Now, let $E_i(n)$ be the collection of all binary strings of length n, even weight, and having an even number of pairs of 1's which are a circular distance of i coordinates apart. For example, $v = (1, 0, 0, 1, 1, 1, 0)$ is in $E_2(7)$ since v has two pairs of 1's, v_4, v_6 and v_6, v_1 which are a circular distance of 2 coordinates apart. Our results on gap forms translate into this context as follows:

Proposition 18 *Suppose $n = 2m + 1$ is prime and $1 \le i \le n - 1$. Then*

$$| E_i(n) | = \begin{cases} 2^{m-1}(2^m + 1) & \textit{if } n \equiv 1, 7 \textit{ (mod 8)} \\ 2^{m-1}(2^m - 1) & \textit{if } n \equiv 3, 5 \textit{ (mod 8)} \end{cases} .$$

Proof By the second supplement to Quadratic Reciprocity

$$(\frac{2}{n}) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \pmod 8 \\ -1 & \text{if } n \equiv 3, 5 \pmod 8 \end{cases} .$$

The result now follows from Proposition 9(2) and Corollary 14. Recall that if $i > m$ then $Q_i = Q_{n-i}$ with $n - i \le m$. Notice that the condition $n \ge (q-1)^r = 1$ of Corollary 14 is trivally satisfied.

■

Proposition 19 *Suppose $n = 2m+1$ is prime and $1 \le i_1 < i_2 \le n-1$ with $i_2 \ne n - i_1$. Then*

$$| E_{i_1}(n) \cap E_{i_2}(n) | = \begin{cases} 2^{m-2}(2^m + 3) & \text{if } n \equiv 1,7 \text{ (mod 8)} \\ 2^{m-2}(2^m - 3) & \text{if } n \equiv 3,5 \text{ (mod 8)} \end{cases} .$$

Proof: This follows from Proposition 15 and Corollary 14.

∎

Proposition 20 *Suppose $n = 2m+1$ is prime and $1 \le i_1 < i_2 < i_3 \le n-1$ with $i_3 - i_2 = i_2 - i_1$ and $i_j \ne n - i_k$ for all j and k. Then*

$$| E_{i_1}(n) \cap E_{i_2}(n) \cap E_{i_3}(n) | = \begin{cases} 2^{m-3}(2^m + 7) & \text{if } n \equiv 1,7 \text{ (mod 8)} \\ 2^{m-3}(2^m - 7) & \text{if } n \equiv 3,5 \text{ (mod 8)} \end{cases} .$$

Proof: This follows from Proposition 16 and Corollary 14.

∎

Example: Consider the case $n = 11$ and $i_1 = 1, i_2 = 2, i_3 = 3$. Proposition 20 gives 100 strings with an even number of pairs of 1's one coordinate apart, an even number of pairs of 1's two coordinates apart and an even number of pairs of 1's three coordinates apart. These 100 are the zero string plus the 11 cyclic permutations of nine basic strings. The basic strings are:

10001000000	10000100000	11000110000
11110011000	11110001100	11101010100
11100101010	11111110100	11111110010

∎

Proposition 21 *For all but a finite number of primes $n = 2m+1$ and $1 \le i_1 < i_2 < \ldots < i_r \le n-1$ with $i_j \ne n - i_k$ for all j and k,*

$$| E_{i_1}(n) \cap E_{i_2}(n) \cap \ldots \cap E_{i_r}(n) | = \begin{cases} 2^{m-r}(2^m + 2^r - 1) & \text{if } n \equiv 1,7 \text{ (mod 8)} \\ 2^{m-r}(2^m - 2^r + 1) & \text{if } n \equiv 3,5 \text{ (mod 8)} \end{cases} .$$

Proof: This follows from Proposition 17 and Corollary 14.

∎

References

[1] E.R. Berlekamp, Algebraic Coding Theory. McGraw-Hill, New York, 1968.

[2] P. Delsarte and J.-M. Goethals, Irreducible binary codes of even dimension. 1970 Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and its Applications, Univ. North Carolina, Chapel Hill NC, 1970, pp. 100-113.

[3] R. Fitzgerald and J. Yucas, Irreducible polynomials over GF(2) with three prescribed coefficients, preprint.

[4] D. Jungnickel, Finite Fields, Bibliographisches Institut & F.A. Brockhaus AG, Mannheim, 1993.

[5] R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997.

Department of Mathematics, Southern Illinois University, Carbondale, IL 62901, Email: rfitzg@math.siu.edu, jyucas@math.siu.edu