Articles and Preprints   Department of Mathematics

2009

Invariants of Trace Forms over Finite Fields of Characteristic 2

Robert W. Fitzgerald

Southern Illinois University Carbondale, rfitzg@math.siu.edu

Recommended Citation

Fitzgerald, Robert W. "Invariants of Trace Forms over Finite Fields of Characteristic 2." (Jan 2009).

Invariants of trace forms over finite fields of characteristic 2

Robert W. Fitzgerald

Abstract

Let K be a finite extension of F_2. We compute the invariants of the quadratic form $Q(x) = \text{tr}_{K/F_2}(x(x^{2^a} + x^{2^b}))$ and so determine the number of zeros in K. This is applied to finding the cross-correlation of certain binary sequences.

Set $F = F_2$ and $K = F_{2^k}$. Let

$$R(x) = \sum_{i=0}^{m} \epsilon_i x^{2^i},$$

with each $\epsilon_i \in K$. Our trace forms are the quadratic forms $Q_R^K : K \to F$ given by $Q_R^K(x) = tr_{K/F}(xR(x))$. These trace forms have appeared in a variety of contexts. They have been used to compute weight enumerators of certain binary codes [1, 2], to construct curves with many rational points and the associated trace codes [9, 4], as part of an authentication scheme [3], and to construct certain binary sequences in [6, 7, 5].

In each of these applications one wants the number of solutions (in K) to $Q_R^K(x) = 0$, denoted by $N(Q_R^K)$. This is easily worked out (see [8], 6.26,6.32) in terms of the standard classification of quadratic forms:

$$N(Q_R^K) = \tfrac{1}{2}(2^k + \Lambda(Q_R^K)\sqrt{2^{k+w}}), \tag{1}$$

where w is the dimension of the radical and

$$\Lambda(Q_R^K) = \begin{cases} 0, & \text{if } Q_R^K \simeq z^2 + \sum_{i=1}^{v} x_i y_i \\ 1, & \text{if } Q_R^K \simeq \sum_{i=1}^{v} x_i y_i \\ -1, & \text{if } Q_R^K \simeq x_1^2 + y_1^2 + \sum_{i=1}^{v} x_i y_i. \end{cases}$$

1

However, there is no simple way to determine the dimension of the radical or the invariant Λ. The one general result is due to Klapper [7] which only covers the case when R consists of a single term. Here we consider the next simplest case: $R(x) = x^{2^a} + x^{2^b}$. The computation depends on a general reduction result which holds for any R with all $\epsilon_i \in \{0, 1\}$. The formula is applied to finding the cross-correlation of certain binary sequences and to finding the size of the intersection of two conics.

We were also motivated by the hope that the formula for this simple case would indicate the formula for general R. However, our expressions for $\dim \mathrm{rad}(Q_R^K)$ and $\Lambda(Q_R^K)$ are quite complicated and suggest that a general result would be too complex to be useful. By way of comparison (and because we will use the result), we give Klapper's result [7] on R with one term:

Theorem 0.1. *Set* $Q_a(x) = tr_{K/F}(x \cdot x^{2^a})$. *Then* $\dim rad(Q_a) = (2a, k)$ *and*

$$
\Lambda(Q_a) = \begin{cases} -1, & \text{if } v_2(2a) < v_2(k) \\ +1, & \text{if } v_2(2a) = v_2(k) \\ 0, & \text{if } v_2(2a) > v_2(k). \end{cases}
$$

Here $v_2(m)$ denotes the highest power of 2 dividing m (that is, the 2-adic valuation). To simplify notation, we will drop the K or the R (or both) from Q_R^K when the choice is clear. If $E = F_{2^e}$ and $G = F_{2^g}$, we will write tr_e for $tr_{E/F}$ and $tr_{e,g}$ for $tr_{E/G}$. Also let $\bar{F}$ denote the algebraic closure of F.

1   Computing the radical

If $E = F_{2^e}$ we will write $\mathrm{rad}_E Q$ for the radical of Q^E. Set

$$
R^* = x^{2^{2b}} + x^{2^{b+a}} + x^{2^{b-a}} + x.
$$

Lemma 1.1.   *1. $x \in rad_{\bar{F}} Q$ iff $R^*(x) = 0$.*

   2. $F_{2^{b+a}}$ and $F_{2^{b-a}}$ are in $rad_{\bar{F}} Q$.

   Proof: (1) is [5] Lemma 11. For (2), if $x \in F_{2^{b+a}}$ then $R^*(x) = (x^{2^{b+a}} + x)^{2^{b-a}} + (x^{2^{b+a}} + x) = 0$. A similar factorization works for $F_{2^{b-a}}$. $\square$

Lemma 1.2. *Let $L = F_{2^n}$ and let $v = v_2(n)$ and $V = 2^v$.*

1. *There exists an irreducible quadratic over L of the form $x^2 + x + r$, where $r \in F_{2^V}$ and $tr_n(r) = 1$.*

2. *If $\alpha \in F_{2^{2n}}$ is a root of irreducible $x^2 + x + r$ then*
$$\alpha^{2^m} = \alpha + p_m(r),$$
where $p_m(r) = r + r^2 + r^4 + \cdots + r^{2^{m-1}}$.

Proof: (1) Pick $r \in F_{2^v}$ with $tr_v(r) = 1$. As $[L : GF(2^v)]$ is odd, $tr_n(r) = 1$ also. By [8] Theorem 3.79, $x^2 + x + r$ is irreducible over L. (2) is a simple induction. $\qquad\square$

In general, set $V_n = 2^{v_2(n)}$, that is, the highest 2-power dividing n.

Lemma 1.3. *Let $e = (b - a, b + a)$.*

1. *Let $\alpha \in F_{2^{2(b-a)}}$ be a root of irreducible $x^2 + x + w$, where $w \in F_{2^{V_{b-a}}}$ and $tr_{b-a}(w) = 1$. Then $\alpha F_{2^e} \subset rad_{\bar{F}} Q$.*

2. *Let $\beta \in F_{2^{2(b+a)}}$ be a root of irreducible $x^2 + x + z$, where $z \in F_{2^{V_{b+a}}}$ and $tr_{b+a}(z) = 1$. Then $\beta F_{2^e} \subset rad_{\bar{F}} Q$.*

Proof: We only prove (1) as the proof of (2) is similar. Let $u \in F_{2^e}$. We compute $R^*(u\alpha)$. Now $u \in GF(2^{b-a})$ so
$$u^{2^{b-a}} = u \qquad u^{2^{2b}} = \left(u^{2^{b-a}}\right)^{2^{b+a}} = u^{2^{b+a}}.$$

Hence using Lemma 1.2 (2) we get

$$
\begin{aligned}
R^*(u\alpha) &= (\alpha + p_{2b}(w))u^{2^{b+a}} + (\alpha + p_{b+a}(w))u^{2^{b+a}} + (\alpha + p_{b-a}(w))u + \alpha u \\
&= \alpha R^*(u) + (p_{2b}(w) + p_{a+b}(w))u^{2^{b+a}} + p_{b-a}(w)u.
\end{aligned}
$$

Now $u \in rad_{\bar{F}} Q$ so $R^*(u) = 0$ by Lemma 1.1. And

$$
\begin{aligned}
p_{b-a}(w) &= w + w^2 + w^4 + \cdots w^{2^{b-a-1}} = tr_{b-a}(w) = 1 \\
p_{2b}(w) + p_{b+a}(w) &= p_{b-a}(w)^{2^{b+a}} = 1.
\end{aligned}
$$

Hence $R^*(u\alpha) = u^{2^{b+a}} + u = 0$, as $u \in F_{2^{b+a}}$ also. $\qquad\square$

Lemma 1.4. *Keep the notation of Lemma 1.3.*

3

1. If $v_2(b+a) \leq v_2(b-a)$ then $rad_{\bar{F}}$ is spanned by $\alpha F_{2^e}, F_{2^{b-a}}$ and $F_{2^{b+a}}$.

2. If $v_2(b+a) > v_2(b-a)$ then $rad_{\bar{F}}$ is spanned by $\beta F_{2^e}, F_{2^{b-a}}$ and $F_{2^{b+a}}$.

Proof: Again we only do (1). Each of the three subspaces are in the radical by Lemmas 1.1 and 1.3. Let $V = 2^{v_2(b-a)}$, the largest 2-power dividing $b - a$. Now α is quadratic over F_{2^V}, so that $\alpha \in F_{2^{V+1}} \setminus F_{2^V}$ while $F_{2^{b-a}}$ and $F_{2^{b+a}}$ are contained in F_{2^ℓ}, where $\ell = lcm(b-a, b+a)$. As $v_2(b+a) \leq v_2(b-a)$, the maximal 2-extension inside F_{2^ℓ} is F_{2^V}. Hence

$$\alpha F_{2^e} \cap \langle F_{2^{b-a}}, F_{2^{b+a}} \rangle = 0.$$

Now

$$\dim F_{2^{b-a}} + F_{2^{b+a}} = (b-a) + (b+a) - \dim F_{2^{b-a}} \cap F_{2^{b+a}} = 2b - e.$$

Thus the span of the three subspaces has dimension $2b$. On the other hand, $\deg R^* = 2^{2b}$ hence the radical has dimension $2b$. So the two are equal. $\square$

Theorem 1.5. *Keep the notation of Lemma 1.3.*

1. *Suppose $v_2(b+a) \leq v_2(b-a)$. Then $rad_K Q =$*

$$\begin{cases} \langle F_{2^{(b-a,k)}}, F_{2^{(b+a,k)}} \rangle & \text{if } v_2(k) \leq v_2(b-a) \\ \langle \alpha F_{2^{(e,k)}}, F_{2^{(b-a,k)}}, F_{2^{(b+a,k)}} \rangle & \text{if } v_2(k) > v_2(b-a). \end{cases}$$

2. *Suppose $v_2(b+a) > v_2(b-a)$. Then $rad_K Q =$*

$$\begin{cases} \langle F_{2^{(b-a,k)}}, F_{2^{(b+a,k)}} \rangle & \text{if } v_2(k) \leq v_2(b+a) \\ \langle \beta F_{2^{(e,k)}}, F_{2^{(b-a,k)}}, F_{2^{(b+a,k)}} \rangle & \text{if } v_2(k) > v_2(b+a). \end{cases}$$

3. *Let $v = \max\{v_2(b-a), v_2(b+a)\}$.*

$$\dim rad_K Q = \begin{cases} (b-a,k) + (b+a,k) - (e,k) & \text{if } v_2(k) \leq v \\ (b-a,k) + (b+a,k) & \text{if } v_2(k) > v. \end{cases}$$

Proof: Both $F_{2^{b-a}} \cap K = F_{2^{(b-a,k)}}$ and $F_{2^{b+a}} \cap K = F_{2^{(b+a,k)}}$ are in $rad_K Q$. Suppose $v_2(b-a) \geq v_2(b+a)$ (the opposite case is similar). Then $(2(b-a), k) = (b-a, k)$. Then

$$\begin{aligned} \alpha F_{2^e} \cap K &\subset F_{2^{2(b-a)}} \cap K \\ &= F_{2^{(2(b-a),k)}} = F_{2^{(b-a,k)}}. \end{aligned}$$

4

But α is quadratic over $F_{2^{b-a}}$ so $\alpha F_{2^e} \cap F_{2^{b-a}} = 0$. Hence $\alpha F_{2^e} \cap K = 0$ and $\mathrm{rad}_K Q$ is spanned by the two fields described.

Now say $v_2(k) > v_2(b-a)$. Again set $V = 2^{v_2(b-a)}$. Then, as α is quadratic over F_{2^V},
$$\alpha \in F_{2^{V+1}} \subset F_{2^{2^{v_2(k)}}} \subset F_{2^k} = K.$$

Hence
$$\alpha F_{2^e} \cap K = \alpha(F_{2^e} \cap K) = \alpha F_{2^{(e,k)}}.$$

This completes the proof of (1). (3) is a simple dimension count. $\qquad\square$

2 Q-value of the radical

Theorem 2.1. $\Lambda(Q) = 0$ *iff* $v_2(b-a) = v_2(b+a) = v_2(k) - 1$.

Proof: $\Lambda(Q) = 0$ iff $Q(\mathrm{rad}(Q)) = 0$. Suppose $v_2(b+a) \leq v_2(b-a)$; the opposite case is similar. First suppose $\gamma \in F_{2^{(b-a,k)}}$, one part of the radical. Then
$$\gamma^{2^{b-a}} = \gamma \qquad \gamma^{2^b+1} = \gamma^{2^a+1}.$$

Thus $Q(\gamma) = 0$. Next say $\gamma \in F_{2^{(b+a,k)}}$, another part of the radical. Then
$$(\gamma^{2^b+1} + \gamma^{2^a+1})^{2^a} = \gamma^{2^{b+a}+2^a} + \gamma^{2^{2a}+2^a} = \gamma^{2^a+1} + (\gamma^{2^a+1})^{2^a}.$$

Thus $Q(\gamma) = \mathrm{tr}_k(\gamma^{2^a+1} + (\gamma^{2^a+1})^{2^a}) = 0$. Hence, by Theorem 1.5, if $v_2(k) \leq v_2(b-a)$ then $Q(\mathrm{rad}Q) = 0$.

We thus now assume $v_2(k) > v_2(b-a)$. The third part of the radical is $\alpha F_{2^{(e,k)}}$ where $\alpha \in K$ is quadratic over F_{2^V}, V the largest 2-power dividing $b-a$. Pick $u \in F_{2^{(e,k)}}$. Note that $u \in F_{2^e} \subset F_{2^{b-a}}$. Hence
$$u^{2^{b-a}} = u \qquad u^{2^b+1} = u^{2^a+1}.$$

Also

$$\begin{aligned}
\alpha^{2^b+1} + \alpha^{2^a+1} &= \alpha(\alpha + p_b(w)) + \alpha(\alpha + p_a(w)) \\
&= \alpha(p_a(w) + p_b(w)) \\
&= \alpha(w^{2^a} + w^{2^{a+1}} + \cdots + w^{2^{2b-1}}) \\
&= \alpha(w + w^2 + \cdots + w^{2^{b-a-1}})^{2^a} \\
&= \alpha(\mathrm{tr}_{b-a}(w))^{2^a} = \alpha.
\end{aligned}$$

Hence $Q(u\alpha) = \mathrm{tr}_k(\alpha u^{2^a+1})$.

Now α and u are in $F_{2^{2(b-a,k)}}$. If $v_2(k) > v_2(b-a)+1$ then $v_2(k) > v_2(2(b-a,k))$ and $[K : F_{2^{2(b-a,k)}}]$ is even. Thus $\mathrm{tr}_k(\alpha u^{2^a+1}) = 0$ and $Q(\mathrm{rad}Q) = 0$ in this case also.

We thus suppose that $v_2(k) = v_2(b-a) + 1$. Then $[K : F_{2^{2(b-a,k)}}]$ is odd. Thus $Q(u\alpha) = \mathrm{tr}_{2(b-a,k)}(\alpha u^{2^a+1})$. Now $w \in F_{2^{(b-a,k)}}$ as $2^{v_2(b-a)}$ divides both $b - a$ and k. Thus α is a quadratic over $F_{2^{(b-a,k)}}$ satisfying $x^2 + x + w$. So $\mathrm{tr}_{2(b-a,k),(b-a,k)}(\alpha) = 1$. We get $Q(u\alpha) = \mathrm{tr}_{(b-a,k)}(u^{2^a+1})$, where $u \in F_{2^{(e,k)}}$ is arbitrary.

If $v_2(b + a) < v_2(b - a)$ then $v_2(e) = v_2(b + a) < v_2(k)$. So $v_2(e, k) < v_2(b - a, k)$. Then $[F_{2^{(b-a,k)}} : F_{2^{(e,k)}}]$ is even and $\mathrm{tr}_{(b-a,k)}(u^{2^a+1}) = 0$. So again $Q(\mathrm{rad}Q) = 0$ in this case.

So lastly assume $v_2(b + a) = v_2(b - a) = v_2(k) - 1$. Then $v_2(e, k) = v_2(b - a, k)$ and we get $Q(u\alpha) = \mathrm{tr}_{(e,k)}(u^{2^a+1})$. Now e divides $b - a$ and $b + a$ so that e divides $2a$. And $b - a = 2^v m$, $b + a = 2^v n$ for some odd m and n. Thus $2a = 2^v(n - m)$. Thus $v_2(2a) \geq v + 1$ and $v_2(a) \geq v_2(e)$. So $e|a$. Thus

$$u^{2^a} = u \quad \text{and} \quad Q(u\alpha) = \mathrm{tr}_{(e,k)}(u^2) = \mathrm{tr}_{(e,k)}(u),$$

which is not zero for all $u \in F_{2^{(e,k)}}$. $\qquad\square$

3 A general reduction result

In this section we will consider more general R, namely, $R(x) = \sum \epsilon_i x^{2^i}$ where each $\epsilon_i \in \{0, 1\}$. The key observation is that $R(x^2) = R(x)^2$ for such R. We write $r(m)$ for $\dim \mathrm{rad}(Q_R^M)$, where $M = F_{2^m}$, and $\Lambda(m)$ for $\Lambda(Q_R^M)$.

We will use the Jacobi symbol $\left(\frac{a}{n}\right)$ and the well-known variation on Euler's Theorem:

$$2^{\frac{p^n-1}{2}} \equiv \left(\frac{2}{p^n}\right) \pmod{p},$$

where p is an odd prime.

Lemma 3.1. *Suppose* $R = \sum \epsilon_i x^{2^i}$ *where each* $\epsilon_i \in \{0,1\}$. *Write* $k = p^n m$ *where* p *is an odd prime and* $(p,m) = 1$. *Then:*

$$\Lambda(k)2^{\frac{r(k)-r(m)}{2}} \equiv \left(\frac{2}{p^n}\right)^m \Lambda(m) \pmod{p}.$$

Proof: Note that $Q(x^2) = \operatorname{tr}_k(x^2 R(x^2)) = \operatorname{tr}_k(xR(x))^2 = Q(x)$. Let $M = F_{2^m}$. If $\gamma \in K \setminus M$ then the cyclotomic class of γ, namely, $\operatorname{cyc}(\gamma) = \{\gamma, \gamma^2, \gamma^4, \ldots\}$, has order $\deg(\gamma)$. Q is constant on $\operatorname{cyc}(\gamma)$. As $F(\gamma)$ is not a subset of M, p divides $\deg(\gamma)$. The zeros of Q in K consist of the zeros of Q in M together with some of the $\operatorname{cyc}(\gamma)$. So

$$
\begin{aligned}
N(Q^K) &\equiv N(Q^M) \pmod{p} \\
2^k + \Lambda(k)2^{(k+r(k))/2} &\equiv 2^m + \Lambda(m)2^{(m+r(m))/2} \pmod{p} \\
\Lambda(k)2^{(k-m)/2} \cdot 2^{(r(k)-r(m))/2} &\equiv \Lambda(m) \pmod{p},
\end{aligned}
$$

as $2^k = 2^{p^n m} \equiv 2^m \pmod{p}$. Lastly,

$$2^{(k-m)/2} = 2^{m(p^n-1)/2} \equiv \left(\frac{2}{p^n}\right)^m \pmod{p},$$

which gives the result. $\square$

Definition 3.2. Let p be an odd prime.

(1) Suppose -1 is a power of 2 modulo p. Set $\eta(p) = 1$ and let $\omega(p)$ be the least positive w such that $2^w \equiv -1 \pmod{p}$.

(2) Suppose -1 is not a power of 2 modulo p. Set $\eta(p) = 0$ and let $\omega(p)$ be the least positive w such that $2^w \equiv 1 \pmod{p}$.

Theorem 3.3. *Suppose* $R = \sum \epsilon_i x^{2^i}$ *where each* $\epsilon_i \in \{0,1\}$. *Write* $k = 2^n p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ *with each* p_i *an odd prime. Set* $\ell = 2^n$ *and* $k^* = k/\ell$. *Then:*

1. $r(k) = \sum_{i=1}^{t} 2s_i \omega(p_i) + r(\ell)$, *for some* s_i.

2.

$$\Lambda(k) = (-1)^{\sum_{i=1}^{t} s_i \eta(p_i)} \left(\frac{2}{k^*}\right)^{\ell} \Lambda(\ell).$$

Proof: We use induction on t. Set $m = k/p_1^{m_1}$. Then, by Lemma 3.1,

$$2^{\frac{r(k)-r(m)}{2}} \equiv \pm 1 \pmod{p}.$$

Then $r(k) = 2s_1\omega(p_1) + r((m)$, for some s_1, by the definition of ω. Then

$$2^{\frac{r(k)-r(m)}{2}} \equiv \begin{cases} (-1)^{s_1}, & \text{if } \eta(p_1) = 1 \\ 1, & \text{if } \eta(p_1) = 0. \end{cases}$$

Hence

$$\Lambda(k) = (-1)^{s_1\eta(p_1)} \left(\frac{2}{p_1^{m_1}}\right)^{m} \Lambda(m).$$

The general result follows by induction. $\qquad\qquad\square$

Corollary 3.4. *Suppose k is odd and $R(x)$ has an odd number of terms. Then $\Lambda(Q_R^K) = 0$.*

Proof: Here $\ell = 1$, $N(Q_R^F) = 1$ and so $\Lambda(1) = 0$. Apply Theorem 3.3. $\qquad\qquad\square$

Example 3.5. We consider $R(x)$ with an even number of terms.

(a) Say $k = 19$. Then $\eta(19) = 1$, $\omega(19) = 8$ and 2 is not a square modulo 19. Then there are only two possibilities:

$$(\dim \mathrm{rad}(Q_R), \Lambda(Q_R)) = (1, -1) \quad \text{or} \quad (19, 1).$$

$R(x) = x^2 + x^4$ gives the first possibility and $R(x) = x^{2^9} + x^{2^{10}}$ gives the second.

Recall that every quadratic form on K arises as $\mathrm{tr}_{K/F}(xR(x))$ for some $R(x)$ with coefficients in K ([4] Theorem 1.2) and so every odd number arises as a $\dim \mathrm{rad}(Q_R^K)$. So the sharp restrictions on $r(k)$ here are a surprising consequence of restricting to those $R(x)$ with all $\epsilon_i \in \{0, 1\}$.

(b) Say $k = 17$. Then $\eta(17) = 1$, $\omega(17) = 4$ and 2 is a square modulo 17. There are three possibilities:

$$(\dim \mathrm{rad}(Q_R), \Lambda(Q_R)) = (1, +1), (9, -1) \quad \text{or} \quad (17, +1).$$

8

Particular examples are $R(x) = x^2 + x^4, x^2 + x^4 + x^8 + x^{32}, x^{256} + x^{512}$, respectively.

(c) Say $k = 21$. Then $\omega(3) = 1$ and $\omega(7) = 3$. Here every odd r, at most 21, can arise as $r = 1 + 2s_1 + 6s_2$. However, a computer search shows there is no R (with all $\epsilon_i = 0, 1$) with $\dim \text{rad}(Q_R^K) = 5$. Thus there are more restrictions on $r(k)$ than those given by Theorem 3.3.

We return to our special case of $R(x) = x^{2^a} + x^{2^b}$.

Lemma 3.6. *Let p be an odd prime and write $k = p^n m$ where $(p, m) = 1$. Set $v^- = v_p(b - a, p)$ and $v^+ = v_p(b + a, p)$. Then*

$$2^{(r(k)-r(m))/2} \equiv \left(\frac{2}{p}\right)^u \pmod{p},$$

where

$$u = \begin{cases} \min\{n, \max\{v^-, v^+\}\}, & \text{if } k \text{ is odd} \\ \min\{n, v^-\} + \min\{n, v^+\}, & \text{if } k \text{ is even}, b \pm a \text{ is odd} \\ 0, & \text{if } k \text{ is even}, b \pm a \text{ is even}. \end{cases}$$

Proof: We will assume $v^- \leq v^+$ (the other case is similar). There are three cases:

$$(i) n \leq v^- \leq v^+ \quad (ii) v^- < n \leq v^+ \quad (iii) v^- \leq v^+ < n.$$

For each of $s = a - b, a + b, e$ we have $(s, k) = p^t(s, m)$, for some t depending on s. The values of t are:

$s =$	$b - a$	$b + a$	e
(i)	n	n	n
(ii)	v^-	n	v^-
(iii)	v^-	v^+	v^-

Further,

$$2^{((s,k)-(s,m))/2} \equiv \left(2^{(p^t-1)/2}\right)^{(s,m)} \equiv \left(\frac{2}{p}\right)^{t(s,m)} \pmod{p}.$$

9

First suppose k is odd so that each (s, m) is odd and $r(k) = (b - a, k) + (b + a, k) - (e, k)$ and $r(m) = (b - a, m) + (b + a, m) - (e, m)$ by Theorem 1.5. We obtain

$$2^{(r(k)-r(m))/2} \equiv \begin{cases} \left(\frac{2}{p}\right)^{3n} & (\text{mod } p), & \text{in case (i)} \\ \left(\frac{2}{p}\right)^{2v^- + n} & (\text{mod } p), & \text{in case (ii)} \\ \left(\frac{2}{p}\right)^{2v^- + v^+} & (\text{mod } p), & \text{in case (iii)}, \end{cases}$$

which gives the desired result.

Next suppose k is even and $b \pm a$ is odd. Again, each (s, m) is odd but now $r(k) = (b - a, k) + (b + a, k)$ and $r(m) = (b - a, m) + (b + a, m)$. We obtain

$$2^{(r(k)-r(m))/2} \equiv \begin{cases} \left(\frac{2}{p}\right)^{2n} & (\text{mod } p), & \text{in case (i)} \\ \left(\frac{2}{p}\right)^{v^- + n} & (\text{mod } p), & \text{in case (ii)} \\ \left(\frac{2}{p}\right)^{v^- + v^+} & (\text{mod } p), & \text{in case (iii)}, \end{cases}$$

which gives the desired result.

Lastly, suppose k is even and $b \pm a$ is even. Then each (s, m) is even and

$$2^{(r(k)-r(m))/2} \equiv \left(\frac{2}{p}\right)^{\sum t(s,m)} \equiv 1 \pmod{p}.$$

$\square$

We summarize:

Theorem 3.7. *Write $k = 2^n m$ where m is odd.*

1. *If k is odd then $\Lambda(k) = \prod\left(\frac{2}{p}\right)$ over odd prime divisors p of k with $v_p(k) + \min\{v_p(k), \max\{v_p(b - a), v_p(b + a)\}\}$ odd.*

2. *If k is even and $b \pm a$ is odd then $\Lambda(k) = \prod\left(\frac{2}{p}\right)\Lambda(2^n)$ over odd prime divisors p of k with $\min\{v_p(k), v_p(b - a)\} + \min\{v_p(k), v_p(b + a)\}$ odd.*

3. *If k is even and $b \pm a$ is even then $\Lambda(k) = \Lambda(2^n)$.*

4 The invariant for 2-power k

We have reduced the computation of $\Lambda(k)$ to the case of a 2-power k. So throughout this section, $k = 2^n$. Set $\ell = k/2$ and $L = F_{2^\ell}$. Then K is a quadratic extension of L. Write $K = L(\delta)$, where $\delta^2 = \delta + y$, with $y \in L$ having $\mathrm{tr}_\ell(y) = 1$. Note that $\mathrm{tr}_k(L) = 0$. We will use the following observation: $v_2(a) \neq v_2(b)$ iff $v_2(b-a) = v_2(b+a)$. And we continue to write v_2^- for $v_2(b-a)$ and v_2^+ for $v_2(b+a)$.

Lemma 4.1. *Let $M = \max\{v_2^-, v_2^+\}$. Let α be as in Lemma 1.3.*

1. *If $n \leq M$ then $Q \equiv 0$ and $\Lambda(k) = +1$.*

2. *If $n = 1 + M$ and $v_2^- \neq v_2^+$ then*
$$\mathrm{rad}(Q) = \langle \alpha F_{2^{2^{v_2^-}}}, F_{2^{2^{v_2^+}}} \rangle \not\subset L.$$

3. *If $n = 1 + M$ and $v_2^- = v_2^+$ then $\Lambda(k) = 0$.*

4. *If $n \geq 2 + M$ and $v_2^- \neq v_2^+$ then*
$$\mathrm{rad}(Q) = \langle \alpha F_{2^{2^{v_2^-}}}, F_{2^{2^{v_2^+}}} \rangle \subset L.$$

5. *If $n \geq 2 + M$ and $v_2^- = v_2^+$ then $\mathrm{rad}(Q) = F_{2^{2^{M+1}}} \subset L$.*

Proof: This follows easily from Theorems 1.5 and 2.1. $\qquad\square$
We thus only need to treat the cases (2), (4) and (5).

Proposition 4.2. *In case (2) we have $\Lambda(k) = -1$.*

Proof: Here we have $v_2(a) = v_2(b)$ and $n = 1 + M$. We suppose $v_2^+ < v_2^-$ (the other case is similar). Thus $v_2(b+a) = v_2(a) + 1 < v_2(b-a)$, $k = 2 \cdot 2^{v_2^-}$ and $\ell = 2^{v_2^-}$. Then $\mathrm{rad}Q = \langle F_{2^{2^{v_2^-}}}, \delta F_{2^{2^{v_2^-}}} \rangle$. Note that $L \subset \mathrm{rad}(Q)$. Now for $u, v \in L$ we have $Q(u + v\delta) = Q(u) + B(u, v\delta) + Q(v\delta) = Q(v\delta)$. Hence $N(Q) = 2^\ell N(Q(v\delta) = 0)$.
We compute:

$$
\begin{aligned}
Q(v\delta) &= \mathrm{tr}_k(v^{2^a+1}(y + \delta + p_a(y)) + v^{2^b+1}(y + \delta + p_b(y))) \\
&= \mathrm{tr}_k(\delta(v^{2^a+1} + v^{2^b+1} + v^{2^a+1}p_a(y) + v^{2^b+1}p_b(y))) \\
&= \mathrm{tr}_\ell(v^{2^a+1} + v^{2^b+1} + v^{2^a+1}p_a(y) + v^{2^b+1}p_b(y)) \\
&= \mathrm{tr}_\ell(v^{2^a+1}p_a(y) + v^{2^b+1}p_b(y)).
\end{aligned}
$$

Here we used that $v, y \in L$ have tr_k equal to 0 and that $Q^L \equiv 0$.

Write $b - a = \ell m$ for some odd m. We have

$$v^{2^b} = v^{2^{a+(b-a)}} \quad = \quad v^{2^a} v^{2^{b-a}} = v^{2^a}$$
$$p_b(y) = p_a(y) + p_{b-a}(y)^{2^a} \quad = \quad p_a(y) + 1.$$

We used that $v \in L$ so that $v^{2^\ell} = v$ and that $p_\ell(y) = \operatorname{tr}_\ell(y) = 1$. Hence $v^{2^b+1} p_b(y) = v^{2^a+1}(1 + p_a(y))$ and $Q(v\delta) = \operatorname{tr}_\ell(v^{2^a+1}) = Q_a^L(v)$. By Klapper's result, Theorem 0.1, as $v_2(\ell) = v_2(b-a) > 1 + v_2(a) = v_2(2a)$, we have $\Lambda(k) = -1$. $\qquad\square$

We now turn to Case (4).

Proposition 4.3. *In case (4) $\Lambda(k) = -1$.*

Proof: Here $v_2(a) = v_2(b)$, call it v and set $V = 2^v$. Also $v_2(b+a) = v+1$, $v_2(b-a) > v+1$ and $v_2(k) \geq v_2(b-a) + 2$. Now

$$2^{sV} \equiv \begin{cases} -1, & \text{if } s \text{ is odd} \\ 1, & \text{if } s \text{ is even} \end{cases} \pmod{2^V + 1}.$$

As a/V and b/V are odd we have that $2^V + 1$ divides both $2^a + 1$ and $2^b + 1$. For each $\beta \in K^*$ of order $2^V + 1$ we have $Q(\beta x) = Q(x)$. As k/V is even, $2^V + 1$ divides $2^k - 1$ and so there are $2^V + 1$ such β's. Thus, counting $x = 0$, we have

$$N(Q) \equiv 1 \pmod{2^V + 1}.$$

Now $k/2V$ is even, $V_{b-a}/2V$ is even and $V_{b+a}/2V$ is odd. Hence

$$2^{(k+V_{b-a}+V_{b+a})/2} \equiv -1 \pmod{2^V + 1},$$

noting that $\dim \operatorname{rad}(Q) = V_{b-a} + V_{b+a}$. Hence

$$N(Q) \quad = \quad \tfrac{1}{2}(2^k + \Lambda(k)\sqrt{2^{k+V_{b-a}+V_{b+a}}})$$
$$\equiv \quad \tfrac{1}{2}(1 + \Lambda(k)(-1)) \pmod{2^V + 1}.$$

Hence $\Lambda(k) = -1$. $\qquad\square$

The one remaining case is Case (5). So for the remainder of this section we assume that $v_2(b-a) = v_2(b+a)$ and that $k \geq 4V_{b-a}$. Now $v_2(a) \neq v_2(b)$ in this case. We will assume $v_2(a) < v_2(b)$ (the opposite case is similar). So $V_{b\pm a} = V_a < V_b$ and $k \geq 4V_a$. We also have $\operatorname{rad}(Q) = F_{2^{2V_a}} \subset L$ by Lemma 4.1.

Lemma 4.4. *Suppose we are in case (5). Let t be the number of $u \in \mathrm{rad}(Q)$ such that $Q(u\delta) = 0$. Then*

$$t = 2^{r-1} + \Lambda(k)2^{r_0-1},$$

where $r = r(k)$ and $r = 2r_0$.

    Proof: Set $W = \mathrm{rad}(Q)$. We have $W \subset L$ and $\dim(L/W)^\perp = (k-r) - (\ell - r) = \ell$ so that $\dim L^\perp = \ell + r$.

    Set $b(x,y) = x^{2^a}y + xy^{2^a} + x^{2^b}y + xy^{2^b}$. Then $B_k(u,v) = \mathrm{tr}_k b(u,v)$. Then, as $\mathrm{tr}_k(L) = 0$, $L \subset L^\perp$. Pick $w_i \in L^\perp$ such that

$$L^\perp = \bigcup_{i=1}^{2^r}(w_i + L).$$

Then pick $v_i \in K \setminus L^\perp$ such that

$$K = L^\perp \cup \bigcup_{i=1}^{2^\ell - 2^r}(v_i + L).$$

Now $Q(v_i + L) = Q(v_i) + B(v_i, L)$ as $Q(L) = 0$. Since $v_i \notin L^\perp$, exactly half of the $B(v_i, \ell)$ are zero. So regardless of the value of $Q(v_i)$, exactly half of the $Q(v_i + \ell)$ are zero. Since the $w_i \in L^\perp$ we have $Q(w_i + L) = Q(w_i)$. Let t be the number of w_i with $Q(w_i) = 0$. Then

$$N(Q) = t \cdot 2^\ell + (2^\ell - 2^r)2^{\ell-1} = 2^{k-1} + 2^\ell(t - 2^{r-1}).$$

Comparing this to the usual formula $t = 2^{r-1} + \Lambda(k)2^{r_0-1}$.   □

Lemma 4.5. *Continue to assume we are in case (5) and that $v_2(a) < v_2(b)$. For $u \in \mathrm{rad}(Q)$ we have*

$$Q(u\delta) = Q^L(u) + \mathrm{tr}_\ell(u^{2^a+1}p_a(\delta) + u^{2^b+1}p_b(\delta)).$$

Further, $Q^L(u) = 0$ for all $u \in \mathrm{rad}(Q)$ except when $k = 4V_a$.

    Proof: We have

$$
\begin{aligned}
Q(u\delta) &= \mathrm{tr}_k(u\delta(u^{2^a}(\delta + p_a(\delta)) + u^{2^b}(\delta + p_b(\delta)))) \\
&= \mathrm{tr}_k(\delta(u^{2^a+1} + u^{2^b+1} + u^{2^a+1}p_a(\delta) + u^{2^b+1}p_b(\delta))) \\
&= \mathrm{tr}_\ell(u^{2^a+1} + u^{2^b+1} + u^{2^a+1}p_a(\delta) + u^{2^b+1}p_b(\delta)) \\
&= Q^L(u) + \mathrm{tr}_\ell(u^{2^a+1}p_a(\delta) + u^{2^b+1}p_b(\delta)).
\end{aligned}
$$

13

As $u \in \mathrm{rad}_k Q \subset L$, we have $u \in \mathrm{rad}_\ell Q$. By Theorem 2.1 this is zero except when $v_2(b - a) = v_2(b + a)$, thus case (5), and $\ell = 2 \cdot 2^{v_2(b-a)}$. Hence $k = 2V_a$. $\qquad\square$

Lemma 4.6. *Let s be a 2-power. Then*

1. $tr_{\ell,s}(p_s(\delta)) = 1$.

2.
$$tr_{\ell,s}(p_{\lambda s}(\delta)) = \begin{cases} 1, & \text{if } \lambda \text{ is odd} \\ 0, & \text{if } \lambda \text{ is even.} \end{cases}$$

Proof: We have

$$\begin{aligned}
tr_{\ell,s}(p_s(\delta)) &= p_s(\delta) + p_s(\delta)^{2^s} + \cdots + p_s(\delta)^{(2^s)^{\ell/s - 1}} \\
&= y + y^2 + \cdots + y^{2^{\ell-1}} \\
&= tr_\ell(y) = 1.
\end{aligned}$$

And for (2)

$$\begin{aligned}
p_{\lambda s}(\delta) &= p_s(\delta) + p_s(\delta)^{2^s} + \cdots + p_s(\delta)^{2^{s(\ell-1)}} \\
tr_{\ell,s}(p_{\lambda s}(\delta)) &= \ell \, tr_{\ell,s}(p_s(\delta)),
\end{aligned}$$

and apply (1). $\qquad\square$

Lemma 4.7. *Continue to assume we are in Case (5) and that $v_2(a) < v_2(b)$. Set $V = V_a$. Let $u \in F_{2^{2V}}$. Then*

$$tr_\ell(u^{2^a+1} p_a(\delta) + u^{2^b+1} p_b(\delta)) = \begin{cases} tr_V(u^{2^V+1}), & \text{if } V_b \geq 4V \\ tr_V(u^{2^V+1}) + tr_{2V}(u), & \text{if } V_b = 2V. \end{cases}$$

Proof: Write $a = Vn$ where $n = 2m + 1$ is odd. Then $a = 2Vm + V$. We have that

$$u^{2^a} = \left(u^{2^{2Vm}}\right)^{2^V} = u^{2^V}.$$

Note that

$$(u^{2^V+1})^{2^V-1} = u^{2^{2V}-1} = 1,$$

if $u \neq 0$. Hence $u^{2^V+1} \in F_{2^V}$. Thus

$$
\begin{aligned}
\mathrm{tr}_\ell(u^{2^a+1}p_a(\delta)) &= \mathrm{tr}_\ell(u^{2^V+1}p_a(\delta)) \\
&= \mathrm{tr}_V(u^{2^V+1}\mathrm{tr}_{\ell,V}(p_a(\delta))) \\
&= \mathrm{tr}_V(u^{2^V+1}),
\end{aligned}
$$

by Lemma 4.6, as a/V is odd.

Next, $b = 2Vm_b$, where m_b is odd iff $V_b = 2V$. Again $u^{2^{2V}} = u$ implies $u^{2^b} = u$. Hence

$$
\mathrm{tr}_\ell(u^{2^b+1}p_b(\delta)) = \mathrm{tr}_\ell(u^2 p_b(\delta)) = \mathrm{tr}_{2V}(u^2\mathrm{tr}_{\ell,2V}(p_b(\delta))),
$$

which is 0 if m_b is even and is $\mathrm{tr}_{2V}(u)$ if m_b is odd. $\qquad\square$

Proposition 4.8. *Continue to assume we are in Case (5) and that $v_2(a) < v_2(b)$. Set $V = V_a$. Then $\Lambda(k) = -1$, except when*

1. *$k \geq 8V$, $V = 1$ and $V_b = 2$ (that is, a is odd and $b \equiv 2 \pmod 4$) in which case $\Lambda(k) = 1$.*

2. *$k = 4V$, $V = 1$ and $V_b \geq 4$ (that is, a is odd and $4|b$) in which case again $\Lambda(k) = 1$.*

Proof: We use Lemma 4.4 to find $\Lambda(k)$. We need to compute t, the number of $u \in \mathrm{rad}(Q)$ with $Q(u\delta) = 0$. First suppose that $k \geq 8V$. For $u \in \mathrm{rad}(Q) = F_{2^{2V}}$ set

$$
q(u) = \mathrm{tr}_V(u^{2^V+1}) \quad \text{and} \quad q^*(u) = q(u) + \mathrm{tr}_{2V}(u).
$$

Then t is $N(q)$ when $V_b \geq 4V$ and $t = N(q^*)$ when $V_b = 2V$, by Lemmas 4.5 and 4.7. Now if V is even then

$$
\begin{aligned}
\mathrm{tr}_{2V}(u) &= \mathrm{tr}_V(u + u^{2^V}) \\
q^*(u) &= \mathrm{tr}_V(u + u^{2^V} + u^{2^V+1}) \\
&= \mathrm{tr}_V((1+u)(1+u^{2^V}) + 1) \\
&= \mathrm{tr}_V((1+u)(1+u)^{2^V}),
\end{aligned}
$$

as V even implies $\mathrm{tr}_V(1) = 0$. Thus $q^*(u) = q(u+1)$ and so $N(q^*) = N(q)$. When $V = 1$ we get $q^*(u+1) = q(u) + 1$ and so $N(q^*) + N(q) = 2^{2V}$.

15

We now compute $N(q)$. The map

$$GF(2^{2V})^* \to GF(2^V)^* \quad \text{by} \quad x \mapsto x^{2^V+1}$$

has kernel of order $2^V + 1$. Hence each image in $GF(2^V)^*$ appears $2^V + 1$ many times. Of the images, $2^{V-1} - 1$ have trace 0. Hence (now including zero)

$$N(q) = (2^V + 1)(2^{V-1} - 1) + 1 = 2^{2V-1} - 2^{V-1}.$$

When $V_b \geq 4V_a$ we have $t = N(q)$ and so $\Lambda(k) = -1$ by Lemma 4.4. When $V_b = 2V_a$ and V is even we have $t = N(q^*) = N(q)$ and again $\Lambda(k) = -1$. When $V_b = 2V_a$ and $V = 1$ then

$$t = N(q^*) = 2^{2V} - N(q) = 2^{2V-1} + 2^{V-1}$$

and so $\Lambda(k) = 1$.

Lastly, suppose $k = 4V$. In this case

$$Q^K(u\delta) = Q^L(u) + \text{tr}_\ell(u^{2^a+1} p_a(\delta) + u^{2^b+1} p_b(\delta)),$$

by Lemma 4.5. Now as in the proof of Lemma 4.7 $u^{2^a+1} = u^{2^V+1} \in F_{2^V}$ and $u^{2^b+1} = u^2$. As $\ell = 2V$ we have $Q^L(u) = \text{tr}_{2V}(u^{2^V+1} + u^2) = \text{tr}_{2V}(u)$. Hence, by Lemma 4.7, $Q^K(u\delta)$ is $q^*(u)$ if $V_b \geq 4V_a$ and $q(u)$ if $V_b = 2V_a$. If V is even then $N(q^*) = N(q)$ so that regardless of the value of V_b/V_a we get the same value of t as above and so $\Lambda(k) = -1$. Finally, if $V = 1$ and $V_b \geq 4V_a$ then $t = N(q^*) = 2^{2V} - N(q)$ so that $\Lambda(k) = 1$. If $V = 1$ and $V_b = 2V_a$ then $t = N(q)$ and $\Lambda(k) = -1$. □

We summarize:

Theorem 4.9. *Let* $k = 2^n$ *and* $M = \max\{v_2(b-a), v_2(b+a)\}$.

1. *If* $n \leq M$ *then* $\Lambda(k) = +1$.

2. *If* $n = 1 + M$ *and* $v_2(b-a) \neq v_2(b+a)$ *then* $\Lambda(k) = -1$.

3. *If* $n = 1 + M$ *and* $v_2(b-a) = v_2(b+a)$ *then* $\Lambda(k) = 0$.

4. *If* $n \geq 2 + M$ *and* $v_2(b-a) \neq v_2(b+a)$ *then* $\Lambda(k) = -1$.

5. *If* $n \geq 2 + M$ *and* $v_2(b-a) = v_2(b+a)$ *then*

    (a) *If* $n = 2$ *and one of* a, b *is odd and the other is* 2 (mod 4) *then* $\Lambda(k) = +1$.

16

(b) *If $n \geq 3$ and one of a, b is odd and the other is divisible by 4 then $\Lambda(k) = +1$.*

(c) *Otherwise, $\Lambda(k) = -1$.*

5 Applications

Here we fix K and a primitive element $\alpha \in K^*$. Set $Q_a(x) = \mathrm{tr}_{K/F}(x \cdot x^{2^a})$, called a gap form in [5]. Let $Q_{a,b}$ denote what has been written as Q_R, namely, $\mathrm{tr}_{K/F}(x \cdot (x^{2^a} + x^{2^b}))$. We consider the sequence

$$\mathbf{S^a} : \qquad s_i^a = Q_a(\alpha^i),$$

for $0 \leq i < 2^k - 1$. These are the pull-backs of the geometric sequences in [7]. The period of $\mathbf{S^a}$ is $\pi_a = (2^k - 1)/(2^a + 1, 2^k - 1)$. In particular, if $(2^a + 1, 2^k - 1) = 1$ then $\mathbf{S^a}$ is an m-sequence. The cross-correlation of two binary sequences $\mathbf{A} = (a_i)$ and $\mathbf{B} = (b_i)$ of period π is:

$$\mathbf{A}.\mathbf{B} = \sum_{i=1}^{\pi} (-1)^{a_i + b_i}.$$

Proposition 5.1. *Suppose $(2^a + 1, 2^k - 1) = d = (2^b + 1, 2^k - 1)$. Then the cross-correlation of $\mathbf{S^a}, \mathbf{S^b}$ is:*

$$\mathbf{S^a}.\mathbf{S^b} = \frac{1}{d}[\Lambda(A_{q,b})2^{(k+r)/2} - 1],$$

where $r = \dim \mathrm{rad}(Q_{a,b})$.

Proof: We have

$$
\begin{aligned}
d(\mathbf{S^a}.\mathbf{S^b}) &= \sum_{i=1}^{2^k - 1} (-1)^{Q_a(\alpha^i) + Q_b(\alpha^i)} \\
&= [N(Q_{a,b}) - 1] - [2^k - N(Q_{a,b})] \\
&= 2N(Q_{a,b}) - 2^k - 1 \\
&= \Lambda(Q_{a,b})2^{(k+r)/2} - 1.
\end{aligned}
$$

$\square$

Example 5.2. Let $a = 1$, $b = 3$ and k be even, not divisible by 6. Then $(2^a + 1, 2^k - 1) = 3 = (2^b + 1, 2^k - 1)$. By Theorem 1.5

$$r(k) = \begin{cases} 2, & \text{if } v_2(k) = 1 \\ 4, & \text{if } v_2(k) = 2 \\ 6, & \text{if } v_2(k) \geq 3. \end{cases}$$

Theorem 3.7 and Theorem 4.9, cases 1,2 and 4 give

$$\Lambda(k) = \Lambda(2^{v_2(k)}) = \begin{cases} +1, & \text{if } v_2(k) = 1 \\ -1, & \text{if } v_2(k) \geq 2. \end{cases}$$

Let $k = 2\ell$. The cross-correlation is then

$$\mathbf{S^1}.\mathbf{S^3} = \begin{cases} +\frac{1}{3}(2^{\ell+1} - 1), & \text{if } v_2(k) = 1 \\ -\frac{1}{3}(2^{\ell+2} + 1), & \text{if } v_2(k) = 2 \\ -\frac{1}{3}(2^{\ell+3} + 1), & \text{if } v_2(k) \geq 3. \end{cases}$$

For a quadratic form q on a vector space V over $F = F_2$, $Z(q)$ denotes the zeros of q and $N(q)$ denotes $|Z(q)|$. Klapper [7] has computed the cardinality of a conic intersected with a hyperplane. Here we compute the intersection of two conics.

Proposition 5.3. Let $q_1, q_2 : V \to F$ be quadratic forms. Then

$$|Z(q_1) \cap Z(q_2)| = \tfrac{1}{2}[N(q_1) + N(q_2) + N(q_1 + q_2) - |V|].$$

Proof: For $w_i \in F$, let $N(w_1, w_2)$ denote the number of $v \in V$ such that $q_i(v) = w_i$, for $i = 1, 2$. Then:

$$
\begin{aligned}
N(0,0) + N(0,1) &= N(q_1) \\
N(0,0) + N(1,0) &= N(q_2) \\
N(0,0) + N(1,1) &= N(q_1 + q_2).
\end{aligned}
$$

Sum the three equations, noting that $N(0,0) + N(0,1) + N(1,0) + N(1,1) = |V|$, to get the desired formula. $\qquad\square$

When $q_1 = Q_a$ and $q_2 = Q_b$ then $q_1 + q_2 = Q_{a,b}$, and so the intersection can be computed.

Example 5.4. Let $a = 3$, $b = 102$ and $k = 2^n \cdot 3 \cdot 5 \cdot 13$. Note that $b - a = 3^2 \cdot 11$ and $b + a = 3 \cdot 5 \cdot 7$. Now $r(k) = 15$ if $n = 0$ and $r(k) = 18$ if $n \geq 1$ by Theorem 1.5. Theorem 3.7 gives $\Lambda(k) = (\frac{2}{13}) = -1$ if $n = 0$ and $\Lambda(k) = (\frac{2}{5})\Lambda(2^n) = -\Lambda(2^n)$ when $n \geq 1$. And Theorem 4.9, cases 1, 3, 5a, c, gives:

$$\Lambda(2^n) = \begin{cases} +1, & \text{if } n = 0, 2 \\ 0, & \text{if } n = 1 \\ -1, & \text{if } n \geq 3. \end{cases}$$

Combining this with Klapper's result, Theorem 0.1, and Equation 1 yields $|Z(Q_a) \cap Z(Q_b)| =:$

$$\begin{cases} \frac{1}{4}[2^k - 2^{(k+15)/2}], & \text{if } n = 0 \\ \frac{1}{4}[2^k + 2^{(k+6)/2}], & \text{if } n = 1 \\ \frac{1}{4}[2^k - 2^{(k+6)/2} + 2^{(k+12)/2} - 2^{(k+18)/2}], & \text{if } n = 2 \\ \frac{1}{4}[2^k - 2^{(k+6)/2} - 2^{(k+12)/2} + 2^{(k+18)/2}], & \text{if } n \geq 3. \end{cases}$$

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, in: 1970 Proc. Second Chapel Hill Conference on Combinatorial Mathematics and Its Applications, Univ. North Carolina, Chapel Hill, NC, 1970, pp. 100–113.

[3] C. Ding, A. Salomaa, P. Solé and X. Tian, Three constructions of authentication/secrecy codes, in: M. Fossorier, T. Høholdt, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 2003), Lecture Notes in Computer Science, vol. 2643, Springer-Verlag, Berlin, 2003, pp. 24–33.

[4] R. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, Finite Fields and Their Applications 11 (2005) 165–181.

[5] R. Fitzgerald and J. Yucas, Pencils of quadratic forms over GF(2) Discrete Math. 283 (2004) 71–79.

[6] K. Khoo, G. Gong and D. R. Stinson, New family of Gold-like sequences, in: IEEE International Symposium on Information Theory 02, 2002, p. 181.

[7] A. Klapper, Cross-correlation of geometric series in characteristic two, Des., Codes, and Cryptogr. 3 (1993) 347–377.

[8] R. Lidl and H. Niederreiter, Finite Fields (second edition), Encyclopedia of Mathematics and Its Applications, vol 20, Cambridge University Press, Cambridge, 1997.

[9] G. van der Geer and M. van der Vlugt, Quadratic forms, generalized Hamming weights of codes and curves with many points, J. Number Theory 59 (1996) 20–36.

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