2003

Irreducible Polynomials over GF(2) with Three Prescribed Coefficients

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

Joseph L. Yucas
Southern Illinois University Carbondale

Published in *Finite Fields and Their Applications*, 9, 286-299.

IRREDUCIBLE POLYNOMIALS OVER GF(2) WITH THREE PRESCRIBED COEFFICIENTS

Robert W. Fitzgerald
Joseph L. Yucas

Southern Illinois University

Abstract. For an odd positive integer n, we determine formulas for the number of irreducible polynomials of degree n over $GF(2)$ in which the coefficients of x^{n-1}, x^{n-2} and x^{n-3} are specified in advance. Formulas for the number of elements in $GF(2^n)$ with the first three traces specified are also given.

Let q be a prime power and let $GF(q)$ be a finite field with q elements. A classical result (see [6, 3.25]) gives the number, $P_q(n)$, of monic, irreducible polynomials of degree n over $GF(q)$:

$$P_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

where μ is the Möbius function. This has been refined several times by counting the number $P_q(n,\epsilon_1,\epsilon_2,\dots,\epsilon_k)$ of monic irreducible polynomials over $GF(q)$ with the first k coefficients being the prescribed values $\epsilon_1,\dots,\epsilon_k$. We are writing polynomials here as

$$p(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n.$$

Carlitz [1] gave a formula for $P_q(n,\epsilon_1)$. Kuz'min [5] extended this to a formula for $P_q(n,\epsilon_1,\epsilon_2)$. This was re-discovered, for the case $q=2$, in [2] which also introduced the connection with higher traces. The same connection was used in [8] to get a formula for $P_q(n,\epsilon_1,\epsilon_2,\epsilon_3)$ when $q=2$ and n is even. We complete this case, getting a formula for $P_q(n,\epsilon_1,\epsilon_2,\epsilon_3)$ when $q=2$ and n is odd. The proof is quite different and depends on computations with quadratic forms.

The higher traces are defined as follows. Let F be any field and let K/F be a separable extension of degree n. Let $\sigma_0,\dots,\sigma_{n-1}$ be the monomorphisms from K into the algebraic closure of F. Then define for $\alpha\in K$:

$$\begin{aligned}
\mathrm{tr}_1(\alpha) &= \sum_{i=0}^{n-1}\sigma_i(\alpha)\\
\mathrm{tr}_2(\alpha) &= \sum_{0\le i<j\le n-1}\sigma_i(\alpha)\sigma_j(\alpha)\\
\mathrm{tr}_3(\alpha) &= \sum_{0\le i<j<k\le n-1}\sigma_i(\alpha)\sigma_j(\alpha)\sigma_k(\alpha)
\end{aligned}$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

In our case ($q = 2$), $\sigma_i(x) = x^{2^i}$.

We fix odd $n = 2m+1$ and set $K = GF(2^n)$. We will only work over $GF(2)$ so we will drop the subscript on the P from $P_2(n, \epsilon_1, \epsilon_2, \epsilon_3)$. Let $F(n, \epsilon_1, \epsilon_2, \epsilon_3)$ denote the number of elements x in K with $\mathrm{tr}_i(x) = \epsilon_i$ for $1 \le i \le 3$ (note that each ϵ_i is 0 or 1). A Möbius inversion-type argument in [8] gives formulas for $P(n, \epsilon_1, \epsilon_2, \epsilon_3)$ in terms of $F(n, \epsilon_1, \epsilon_2, \epsilon_3)$ so we will concentrate on evaluating the F's.

1. Identities.

Set $Q = \mathrm{tr}_2 + \mathrm{tr}_3$. We also define maps $B_i : K \times K \to F$ as follows:

$$\begin{aligned}
B_2(\alpha, \beta) &= \mathrm{tr}_2(\alpha + \beta) + \mathrm{tr}_2(\alpha) + \mathrm{tr}_2(\beta)\\
B_3(\alpha, \beta) &= \mathrm{tr}_3(\alpha + \beta) + \mathrm{tr}_3(\alpha) + \mathrm{tr}_3(\beta)\\
B_Q(\alpha, \beta) &= Q(\alpha + \beta) + Q(\alpha) + Q(\beta) = B_2(\alpha, \beta) + B_3(\alpha, \beta).
\end{aligned}$$

Special cases of the following are known, see [4, 0.2] and [8, Proposition 10].

Lemma 1.1. *(1)* $B_2(\alpha, \beta) = tr_1(\alpha)tr_1(\beta) + tr_1(\alpha\beta)$.

(2) $B_3(\alpha, \beta) = tr_2(\alpha)tr_1(\beta) + tr_1(\alpha)tr_2(\beta) + tr_1(\alpha\beta^2 + \alpha^2\beta) + tr_1(\alpha\beta)tr_1(\alpha + \beta)$.

Proof. (1) To save on superscripts, we set $x_i = x^{2^i}$. Then

$$\begin{aligned}
B_2(\alpha, \beta) &= \sum_{0 \le i < j \le n-1} [(\alpha + \beta)_i(\alpha + \beta)_j + \alpha_i\alpha_j + \beta_i\beta_j]\\
&= \sum_{i \ne j} \alpha_i\beta_j\\
&= \sum_{i=0}^{n-1} \alpha_i \sum_{j \ne i} \beta_j\\
&= \sum_{i=0}^{n-1} \alpha_i(\mathrm{tr}_1(\beta) + \beta_i)\\
&= \mathrm{tr}_1(\alpha)\mathrm{tr}_1(\beta) + \mathrm{tr}_1(\alpha\beta).
\end{aligned}$$

(2)

$$
\begin{aligned}
B_3(\alpha,\beta) &= \sum_{0\le i<j<k\le n-1} [\alpha_i\alpha_j\beta_k + \alpha_i\beta_j\alpha_k + \beta_i\alpha_j\alpha_k + \alpha_i\beta_j\beta_k + \beta_i\alpha_j\beta_k + \beta_i\beta_j\alpha_k] \\
&= \sum_{k=0}^{n-1}\Big(\sum_{\substack{i<j\\ i,j\neq k}} \alpha_i\alpha_j\Big)\beta_k + \sum_{i<j}\Big(\sum_{k\neq i,j}\alpha_k\Big)\beta_i\beta_j \\
&= \sum_{k=0}^{n-1}\big[\mathrm{tr}_2(\alpha) + \alpha_k\sum_{i\neq k}\alpha_i\big]\beta_k + \sum_{i<j}\big[\mathrm{tr}_1(\alpha)+\alpha_i+\alpha_j\big]\beta_i\beta_j \\
&= \mathrm{tr}_2(\alpha)\mathrm{tr}_1(\beta) + \mathrm{tr}_1(\alpha)\mathrm{tr}_1(\alpha\beta) + \mathrm{tr}_1(\alpha^2\beta) \\
&+ \mathrm{tr}_1(\alpha)\mathrm{tr}_2(\beta) + \mathrm{tr}_1(\alpha\beta^2) + \mathrm{tr}_1(\alpha\beta)\mathrm{tr}_1(\beta) \\
&= \mathrm{tr}_2(\alpha)\mathrm{tr}_1(\beta) + \mathrm{tr}_1(\alpha)\mathrm{tr}_2(\beta) + \mathrm{tr}_1(\alpha\beta^2+\alpha^2\beta) + \mathrm{tr}_1(\alpha\beta)\mathrm{tr}_1(\alpha+\beta).
\end{aligned}
$$

□

Recall that K is a finite field of characteristic 2. In particular, $K = K^2$. Set $K_1 = \ker(\mathrm{tr}_1)$.

Definition. Let $\psi_2 : K_1 \to K$ be $\psi_2(\alpha) = \sqrt{\alpha} + \alpha^2$. Let $\psi_3 : K_1 \to K$ be $\psi_3(\alpha) = \sqrt{\alpha} + \alpha + \alpha^2$.

Lemma 1.2. *For $\alpha, \beta \in K_1$ we have:*

1. *$B_2(\alpha,\beta) = tr_1(\alpha\beta)$.*
2. *$B_3(\alpha,\beta) = tr_1(\psi_2(\alpha)\beta)$*
3. *$B_Q(\alpha,\beta) = tr_1(\psi_3(\alpha)\beta)$.*

Proof. (1) is clear form (1.1). For (2), (1.1) gives

$$
\begin{aligned}
B_3(\alpha,\beta) &= \mathrm{tr}_1(\alpha^2\beta + \alpha\beta^2) \\
&= \mathrm{tr}_1(\alpha^2\beta + (\sqrt{\alpha}\beta)^2) \\
&= \mathrm{tr}_1(\alpha^2\beta + \sqrt{\alpha}\beta) \\
&= \mathrm{tr}_1(\psi_2(\alpha)\beta).
\end{aligned}
$$

And lastly, $B_Q(\alpha,\beta) = \mathrm{tr}_1(\alpha\beta) + \mathrm{tr}_1(\psi_2(\alpha)\beta)$. □

We note that it is only for $GF(2)$ that ψ_2 and ψ_3 are linear.

Lemma 1.3.

1. *$\psi_2 : K_1 \to K_1$ is an isomorphism.*
2. *If 3 does not divide n then $\psi_3 : K_1 \to K_1$ is an isomorphism.*
3. *If 3 does divide n then $\ker(\psi_3)$ has order 4.*

Proof. (1) Since $\mathrm{tr}_1(\alpha) = \mathrm{tr}_1(\alpha^2)$ we have that ψ_2 maps into K_1. Say $\alpha \in \ker\psi_2$ and let $\beta^2 = \alpha$. Then $\beta + \beta^4 = 0$. But $x + x^4 = x(x+1)(x^2+x+1)$ and x^2+x+1 has no roots in K as $[K : F]$ is odd. Hence only 0 and 1 are sent to 0 by ψ_2 and $1 \notin K_1$. Thus ψ_2 is injective and so an isomorphism.

(2) First $\mathrm{tr}_1(\sqrt{\alpha} + \alpha + \alpha^2) = \mathrm{tr}_1(\alpha)$, so ψ_3 maps K_1 into K_1. Say $\alpha \in \ker\psi_3$ and let $\beta^2 = \alpha$. Then $\beta + \beta^2 + \beta^4 = 0$. But $x + x^2 + x^4 = x(1 + x + x^3)$ and the cubic has no roots in K if 3 does not divide n. So ψ_3 is an isomorphism.

(3) As above, $\ker(\psi_3)$ consists of the roots of $x + x^2 + x^4$ and so has order 4. □

Lemma 1.4. *For $\alpha \in K_1$, $tr_3(\alpha) = tr_1(\alpha^3)$.*

Proof. Again let α_i denote α^{2^i}. We first note that

$$\mathrm{tr}_3(\alpha) = \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \mathrm{tr}_1(\alpha\alpha_i\alpha_j).$$

Namely, each term $\alpha_a\alpha_b\alpha_c$ occurs three times, once each in the sums for $\mathrm{tr}_1(\alpha\alpha_{b-a}\alpha_{c-a})$, $\mathrm{tr}_1(\alpha\alpha_{c-b}\alpha_{a+n-b})$ and $\mathrm{tr}_1(\alpha\alpha_{a+n-c}\alpha_{b+n-c})$. Thus

$$\begin{aligned}
\mathrm{tr}_3(\alpha) &= \mathrm{tr}_1(\alpha \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \alpha_i\alpha_j) \\
&= \mathrm{tr}_1(\alpha(\mathrm{tr}_2(\alpha) - \alpha \sum_{i=1}^{n-1} \alpha_i)) \\
&= \mathrm{tr}_1(\alpha(\mathrm{tr}_2(\alpha) - \alpha(\mathrm{tr}_1(\alpha) - \alpha))) \\
&= \mathrm{tr}_1(\alpha\mathrm{tr}_2(\alpha) + \alpha^3) \quad \text{since } \alpha \in K_1 \\
&= \mathrm{tr}_2(\alpha)\mathrm{tr}_1(\alpha) + \mathrm{tr}_1(\alpha^3) = \mathrm{tr}_1(\alpha^3).
\end{aligned}$$

□

2. Quadratic forms.

Over any field of characteristic 2 a *quadratic form* on an F-vector space V is a map $q : V \to F$ such that (1) $q(\lambda v) = \lambda^2 q(v)$ and (2) $b_q(v, w) \equiv q(v + w) - q(v) - q(w)$ is a symmetric bilinear form. We say q is *non-degenerate* if b_q is, namely, $b_q(v, w) = 0$ for all $w \in V$ implies $v = 0$. Note that b_q is *alternating*, namely that $b_q(v, v) = 0$ for all $v \in V$.

The non-degenerate , alternating, symmetric bilinear forms are necessarily even dimensional and have a symplectic basis $\{e_i, f_i\}$, $1 \le i \le m$, meaning

$$\begin{aligned}
b_q(e_i, e_j) &= 0 \\
b_q(e_i, f_j) &= \delta_{ij} \\
b_q(f_i, f_j) &= 0.
\end{aligned}$$

See [7, Chapter 9, Section 4] for further details.

We continue to assume $F = GF(2)$, since only in this case is condition (1) of a quadratic form satisfied by tr_3.

Lemma 2.1.

(1) *tr_2, tr_3 and Q are quadratic forms $K_1 \to GF(2)$.*
(2) *tr_2 and tr_3 are non-degenerate.*
(3) *Q is non-degenerate if 3 does not divide n. If 3 does divide n then the radical of Q is $C \equiv \ker \psi_3$ and Q is non-degenerate on K_1/C.*

Proof. (1) follows from (1.2). The trace form, $\alpha, \beta \to \mathrm{tr}_1(\alpha\beta)$ is non-degenerate by [6, 2.24]. Hence (2) and (3) follow from (1.3). □

We use the notation $\mathrm{sp}(S)$ for the linear span of a set S.

Lemma 2.2. *Let q be a non-degenerate $2m$-dimensional quadratic form over $GF(2)$. Set $B = b_q$. Suppose U is an m-dimensional subspace with $B(u, u') = 0$ for all $u, u' \in U$. Then any basis of U can be extended to a symplectic basis $\{u_i, v_i\}$, $1 \le i \le m$. Moreover, v_1 can be taken to be any vector in $sp(u_2, \ldots, u_m)^{\perp} \setminus U$.*

Proof. Let $u_1, \ldots, u_m$ be a basis of U. Now $U \subset \mathrm{sp}(u_2, \ldots, u_m)^{\perp}$ and $\dim \mathrm{sp}(u_2, \ldots, u_m)^{\perp}$ is $m+1$. So write

$$\mathrm{sp}(u_2, \ldots, u_m)^{\perp} = U \oplus v,$$

for some v. Set $v_1 = v$. Then $B(u_i, v_1) = 0$ for all $i \ge 2$. Also $B(u_1, v_1) = 1$, else $v_1 \in U^{\perp} = U$, a contradiction.

Suppose we have constructed $v_1, \ldots v_k$ with $B(v_i, v_j) = 0$ and $B(u_i, v_j) = \delta_{ij}$. As before,

$$\mathrm{sp}(u_1, \ldots, u_k, u_{k+2}, \ldots, u_m)^{\perp} = U \oplus r,$$

for some r. Set $S = \{i : 1 \le i \le k \quad B(v_i, r) = 1\}$ and let

$$v_{k+1} = r + \sum_{i \in S} u_i.$$

We check that this works. $B(u_i, v_{k+1}) = 0$ for all $i \ne k+1$. Then $B(u_{k+1}, v_{k+1}) = 1$, else $v_{k+1} \in U^{\perp} = U$ while $r \notin U$. If $j \notin S$ then

$$B(v_j, v_{k+1}) = B(v_j, r) + \sum_{i \in S} B(v_i, u_j) = 0.$$

If $j \in S$ then

$$\begin{aligned} B(v_j, v_{k+1}) &= B(v_j, r) + \sum_{i \in S} B(v_i, u_j) \\ &= B(v_j, r) + B(v_j, u_j) = 1 + 1 = 0. \end{aligned}$$

□

Let $N(f = a)$ denote the number of solutions to $f = a$. Let $mH = x_1 y_1 + \cdots + x_m y_m$. We will use:

$$N(mH = \alpha) = \begin{cases} 2^{2m-1} + 2^{m-1}, & \text{if } \alpha = 0 \\ 2^{2m-1} - 2^{m-1}, & \text{if } \alpha = 1. \end{cases} \tag{2.3}$$

This is [6, 6.32]. It can be proven directly by a simple induction argument.

Lemma 2.4. *Let q be a $2m$-dimensional, non-degenerate quadratic form. Let U be an m-dimensional space with $b_q(u, u') = 0$ for all $u, u' \in U$. Suppose $\{u_1, \dots, u_m\}$ is a basis of U with $q(u_1) = 1$ and $q(u_i) = 0$ for $2 \le i \le m$. Let $v_1 \in sp(u_2, \dots, u_m)^\perp \setminus U$. Then:*

$$N(q=0) = \begin{cases} 2^{2m-1} + 2^{m-1}, & \text{if } q(v_1) = 0 \\ 2^{2m-1} - 2^{m-1}, & \text{if } q(v_1) = 1. \end{cases}$$

Proof. This can be deduced from [6, 6.32] but a direct proof is no more difficult. Extend $\{u_1, \dots, u_m, v_1\}$ to a symplectic basis $\{u_i, v_i\}$, which is possible by (2.2). For $z = \sum x_i u_i + \sum y_i v_i$ we have:

$$q(z) = x_1^2 + \sum_{i=1}^m x_i y_i + \sum_{i=1}^m q(v_i) y_i^2.$$

Note that x^2 and x are equal as functions over $GF(2)$ so that

$$q(z) = x_1 + x_1 y_1 + q(v_1) y_1 + \sum_{i=2}^m (x_i + q(v_i)) y_i.$$

If $q(v_1) = 0$ then $q(z) = x_1(1 + y_1) + \sum (x_i + q(v_i)) y_i$. Hence $N(q = 0) = N(mH = 0)$. Apply (2.3). If $q(v_1) = 1$ then

$$q(z) = 1 + (1 + x_1)(1 + y_1) + \sum_{i=2}^m (x_i + q(v_i)) y_i.$$

So $N(q = 0) = N(mH = 1)$. Apply (2.3). □

We note that $q(v_1)$ is the Arf invariant of q, see [7, Chapter 9, section 4].

For $i = 2, 3, Q$ write $\text{perp}_i(S)$ for $\{v \in K_1 : B_i(v, s) = 0 \quad \text{for all } s \in S\}$.

We will construct, in the next section, elements $u_1, \dots, u_m, x_1, y_2, z_1 \in K_1$ such that

(1) $B_2(u_i, u_j) = 0 = B_3(u_i, u_j)$ for all $i, j = 1, \dots, m$.
(2) $\text{tr}_2(u_1) = \text{tr}_3(u_2) = 1$.
(3) $\text{tr}_3(u_1) = \text{tr}_2(u_2) = 0$.
(4) $\text{tr}_2(u_i) = 0 = \text{tr}_3(u_i)$ for all $3 \le i \le m$.
(5) $x_1 \in \text{perp}_2(u_2, \dots, u_m) \setminus U$, where U is the span of $u_1, \dots, u_m$.
(6) $y_2 \in \text{perp}_3(u_1, u_3, \dots, u_m) \setminus U$.
(7) $z_1 \in \text{perp}_Q(u_2, \dots, u_m) \setminus U$.

Now Q is degenerate if 3 divides n (2.1). Let $\bar{v}$ denote $v + C$ and let $\bar{Q}$ denote the map induced by Q on $\bar{K}_1 = K_1/C$. When 3 divides n we require two additional properties of our construction:

(8) $|C \cap U| = 2$ with the non-zero element γ of $C \cap U$ satisfying $\gamma + u_1 \in \text{sp}(u_2, \dots u_m)$.
(9) $\bar{z}_2 \in \text{perp}_{\bar{Q}}(\bar{u}_3, \dots, \bar{u}_m) \setminus \bar{U}$.

Proposition 2.5. *Let $n \geq 7$ and assume we have constructed elements in K_1 satisfying (1)-(9). If 3 does not divide n then:*

$$\begin{aligned}
F(n,0,0,0) &= 2^{2m-2} + 3 \cdot 2^{m-2} - (tr_2(x_1) + tr_3(y_2) + Q(z_1))2^{m-1} \\
F(n,0,0,1) &= 2^{2m-2} - 2^{m-2} + (-tr_2(x_1) + tr_3(y_2) + Q(z_1))2^{m-1} \\
F(n,0,1,0) &= 2^{2m-2} - 2^{m-2} + (tr_2(x_1) - tr_3(y_2) + Q(z_1))2^{m-1} \\
F(n,0,1,1) &= 2^{2m-2} - 2^{m-2} + (tr_2(x_1) + tr_3(y_2) - Q(z_1))2^{m-1}.
\end{aligned}$$

If 3 divides n then:

$$\begin{aligned}
F(n,0,0,0) &= 2^{2m-2} + 2^{m} - (tr_2(x_1) + tr_3(y_2) + 2\bar{Q}(\bar{z}_2))2^{m-1} \\
F(n,0,0,1) &= 2^{2m-2} - 2^{m-1} + (-tr_2(x_1) + tr_3(y_2) + 2\bar{Q}(\bar{z}_2))2^{m-1} \\
F(n,0,1,0) &= 2^{2m-2} - 2^{m-1} + (tr_2(x_1) - tr_3(y_2) + 2\bar{Q}(\bar{z}_2))2^{m-1} \\
F(n,0,1,1) &= 2^{2m-2} + (tr_2(x_1) + tr_3(y_2) - 2\bar{Q}(\bar{z}_2))2^{m-1}.
\end{aligned}$$

Proof. (1) We first note that

$$\begin{aligned}
\{u_1, \ldots, u_m, x_1\} &\quad \text{meets the hypotheses of (2.4) for } q = \mathrm{tr}_2 \\
\{u_2, u_1, u_3, \ldots, u_m, y_2\} &\quad \text{meets the hypotheses of (2.4) for } q = \mathrm{tr}_3 \\
\{u_1, u_1 + u_2, u_3 \ldots, u_m, z_1\} &\quad \text{meets the hypotheses of (2.4) for } q = Q.
\end{aligned}$$

Applying (2.4) yields

$$\begin{aligned}
F(n,0,0,0) + F(n,0,0,1) = N(\mathrm{tr}_2 = 0) &= 2^{2m-1} + 2^{m-1} - 2\mathrm{tr}_2(x_1)2^{m-1} \\
F(n,0,0,0) + F(n,0,1,0) = N(\mathrm{tr}_3 = 0) &= 2^{2m-1} + 2^{m-1} - 2\mathrm{tr}_3(y_2)2^{m-1} \\
F(n,0,0,0) + F(n,0,1,1) = N(Q = 0) &= 2^{2m-1} + 2^{m-1} - 2Q(z_1)2^{m-1} \\
F(n,0,0,0) + F(n,0,0,1) + F(n,0,1,0) + F(n,0,1,1) &= 2^{2m}.
\end{aligned}$$

The sum of the first three minus the fourth gives a formula for $2F(n,0,0,0)$. The others are easily found.

(2) Here Q is degenerate. Note that $\{\bar{u}_1, \bar{u}_3, \ldots, \bar{u}_m, \bar{z}_2\}$ meets the hypothesis of (2.4) for $q = \bar{Q}$. The two variables associated to C can take any value without affecting the value of Q. Hence

$$\begin{aligned}
N(Q = 0) &= 4N(\bar{Q} = 0) \\
&= 4(2^{2(m-1)-1} + 2^{(m-1)-1} - 2\bar{Q}(\bar{z}_2)2^{(m-1)-1}) \\
&= 2^{2m-1} + 2^{m} - 2\bar{Q}(\bar{z}_2)2^{m}.
\end{aligned}$$

Replace the right-hand side of the third equation above with this expression and solve. □

To complete the count we have:

Lemma 2.6.

$$F(n,0,\epsilon_2,\epsilon_3) = \begin{cases} F(n,1,\epsilon_2,\epsilon_2+\epsilon_3), & \text{if } m \text{ is even} \\ F(n,1,1+\epsilon_2,1+\epsilon_2+\epsilon_3), & \text{if } m \text{ is odd.} \end{cases}$$

Proof. From (1.1) we have for $\alpha \in K_1$

$$\begin{aligned} B_2(1,\alpha) &= \mathrm{tr}_1(1\cdot\alpha) + \mathrm{tr}_1(1)\mathrm{tr}_1(\alpha) = 0. \\ B_3(1,\alpha) &= \mathrm{tr}_2(1)\mathrm{tr}_1(\alpha) + \mathrm{tr}_2(\alpha)\mathrm{tr}_1(1) + \mathrm{tr}_1(\alpha^2+\alpha) \\ &= \mathrm{tr}_2(\alpha). \end{aligned}$$

Hence

$$\begin{aligned} \mathrm{tr}_2(1+\alpha) &= \mathrm{tr}_2(1) + \mathrm{tr}_2(\alpha) \\ \mathrm{tr}_3(1+\alpha) &= \mathrm{tr}_3(1) + \mathrm{tr}_2(\alpha) + \mathrm{tr}_3(\alpha). \end{aligned}$$

Since

$$\mathrm{tr}_2(1) \equiv \binom{n}{2} \pmod 2 \quad \text{and} \quad \mathrm{tr}_3(1) \equiv \binom{n}{3} \pmod 2,$$

we have $\mathrm{tr}_2(1) = 1$ iff $\mathrm{tr}_3(1) = 1$ iff m is odd. The result follows. □

3. The construction.

We will now give an explicit construction of $u_1,\dots,u_m, x_1, y_2, z_1$ and $\bar{z}_2$. Let $B = \{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\}$ be a self-dual normal basis for K, see [3, 5.2.1] for the existence of such a basis. Here self-dual means that

$$\mathrm{tr}_1(\alpha^{2^i}\alpha^{2^j}) = \delta_{ij}.$$

We will use:

Proposition 3.1. *Let $\gamma = c_0\alpha + c_1\alpha^2 + \cdots + c_{n-1}\alpha^{2^{n-1}} \in K_1$.*

(1) *$tr_1(\gamma) \equiv c_0 + c_1 + \cdots + c_{n-1} \pmod 2$ is zero.*
(2) *$tr_2(\gamma) \equiv \frac{1}{2}(c_0 + c_1 + \cdots + c_{n-1}) \pmod 2$.*
(3) *$tr_3(\gamma) \equiv c_{n-1}c_0 + c_0c_1 + c_1c_2 + \cdots + c_{n-2}c_{n-1} \pmod 2$.*

Proof. (1) is [2, Lemma 9]. (2) is implicit in [2]. Namely, [2, Theorem 5] gives

$$\mathrm{tr}_2(\gamma) \equiv \sum_{0\le i<j<n} c_ic_j \pmod 2.$$

Now follow the proof of [2, Lemma 7]. Let k be the number of c_i equal to 1. The sum $\sum c_i c_j$ counts the number of pairs of 1's in the string $c_0 c_1 \dots c_{n-1}$. Thus

$$\sum_{0\le i<j<n} c_i c_j = \binom{k}{2}.$$

Since k is even by (1), we have $\mathrm{tr}_2(\gamma) = 0$ iff $k \equiv 0 \pmod 4$, which yields (2).

For (3) we have by (1.4)

$$\begin{aligned}\mathrm{tr}_3(\gamma) &= \mathrm{tr}_1(\gamma^3) = \mathrm{tr}_1(\gamma\gamma^2)\\ &= \mathrm{tr}_1((c_0\alpha + c_1\alpha^2 + \dots + c_{n-1}\alpha^{2^{n-1}})(c_{n-1}\alpha + c_0\alpha^2 + \dots + c_{n-2}\alpha^{2^{n-1}})).\end{aligned}$$

Since $\mathrm{tr}_1(\alpha^{2^i}\alpha^{2^j}) = \delta_{ij}$ we have the result. $\square$

Proposition 3.2. *Let* $\beta = b_0\alpha + b_1\alpha^2 + \dots + b_{n-1}\alpha^{2^{n-1}}$ *and* $\gamma = c_0\alpha + c_1\alpha^2 + \dots + c_{n-1}\alpha^{2^{n-1}}$ *be in* K_1.

(1) $B_2(\beta,\gamma) = b_0c_0 + b_1c_1 + \dots + b_{n-1}c_{n-1} \pmod 2$.
(2) $B_3(\beta,\gamma) = b_0(c_{n-1} + c_1) + b_1(c_0 + c_2) + \dots + b_{n-1}(c_{n-2} + c_0) \pmod 2$.
(3) $B_Q(\beta,\gamma) = b_0(c_{n-1} + c_0 + c_1) + b_1(c_0 + c_1 + c_2) + \dots + b_{n-1}(c_{n-2} + c_{n-1} + c_0) \pmod 2$.

Proof. From (1.1), $B_2(\beta,\gamma) = \mathrm{tr}_1(\beta\gamma)$, $B_3(\beta,\gamma) = \mathrm{tr}_1(\beta\gamma^2 + \beta^2\gamma)$ and $B_Q(\beta,\gamma) = \mathrm{tr}_1(\beta\gamma + \beta\gamma^2 + \beta^2\gamma)$. Now compute using the fact that $\mathrm{tr}_1(\alpha^{2^i}\alpha^{2^j}) = \delta_{ij}$. $\square$

For $\gamma = c_0\alpha + c_1\alpha^2 + \dots + c_{n-1}\alpha^{2^{n-1}}$ we abuse notation and write $\gamma = (c_0c_1\dots c_{n-1})$. We use $*$ for concatenation and $n(s)$ for the concatenation of n copies of (s). We assume $n \ge 7$.

Let

$$\begin{aligned}
u_1 &= (00001) * (n-6)(0) * (1)\\
u_2 &= (1111) * (n-4)(0)\\
u_j &= (1001) * (j-3)(0) * (1) * (n-2j)(0) * (1) * (j-3)(0), \quad j = 3, \dots, m\\
x_1 &= (1100) * k(1) * (n-k-4)(0), \quad k = 2\left\lfloor \frac{n-3}{4} \right\rfloor\\
y_2 &= \begin{cases} (11101) * (2t-1)(1001), & \text{if } n = 8t+1\\ (110) * 2t(1100), & \text{if } n = 8t+3\\ (11101) * 2t(1001), & \text{if } n = 8t+5\\ (101) * (2t+1)(1100), & \text{if } n = 8t+7.\end{cases}
\end{aligned}$$

If 3 does not divide n then set

$$z_1 = \begin{cases} (1001) * (2t-1)(101) * 2t(100), & \text{if } n = 12t+1\\ (00) * (2t+1)(101) * 2t(001), & \text{if } n = 12t+5\\ (0000) * (2t+1)(110) * 2t(010), & \text{if } n = 12t+7\\ (11010) * (2t+1)(110) * (2t+1)(100), & \text{if } n = 12t+11.\end{cases}$$

If 3 does divide n then set

$$z_2 = \begin{cases} (000) * 2t(011) * 2t(010), & \text{if } n = 12t+3 \\ (000010) * 2t(110) * (2t+1)(100), & \text{if } n = 12t+9. \end{cases}$$

Proposition 3.3. *Let $n \geq 7$.*

(1) *$u_1, \ldots, u_m, x_1, y_2$ and z_1 satisfy conditions (1)-(7) of the last section.*

(2)
$$tr_2(x_1) = tr_3(y_2) = \begin{cases} 0, & \text{if } m \equiv 0,3 \pmod 4 \\ 1, & \text{if } m \equiv 1,2 \pmod 4. \end{cases}$$

(3) *If 3 does not divide n then $Q(z_1) = tr_2(x_1)$.*

(4) *If 3 does divide n then conditions (8) and (9) of the previous section hold. And $\bar{Q}(\bar{z}_2) = tr_2(x_1) + 1$.*

Proof. (1), (2) and (3) consist of several easy computations using (3.1) and (3.2). We do the computations involving x_1, namely condition (5) of the previous section and statement (2). Notice that $u_1 = \alpha^{16} + \alpha^{2^{n-1}}$, $u_2 = \alpha + \alpha^2 + \alpha^4 + \alpha^8$, $u_j = \alpha + \alpha^8 + \alpha^{2^{j+1}} + \alpha^{2^{n-j+2}}$, for $j = 3, \ldots, m$, and

$$x_1 = \alpha + \alpha^2 + \sum_{i=4}^{m+1} \alpha^{2^i} + \epsilon\alpha^{2^{m+2}},$$

where

$$\epsilon = \begin{cases} 0, & \text{if } m \text{ is even} \\ 1, & \text{if } m \text{ is odd.} \end{cases}$$

Now, x_1 and u_1 match only at α^{16} so by (3.2), $B_2(u_1, x_1) = 1$. In particular, $x_1 \notin U$. Next, x_1 and u_2 match only at α and α^2 so that $B_2(u_2, x_1) = 0$. Also, x_1 and u_j, $3 \leq j \leq m$, match only at α and $\alpha^{2^{j+1}}$ so that $B_2(u_j, x_1) = 0$. This proves condition (5). Finally, by (3.1),

$$\begin{aligned} \mathrm{tr}_2(x_1) &\equiv \tfrac{1}{2}(1 + 1 + (m-2) + \epsilon) \equiv \tfrac{1}{2}(m + \epsilon) \pmod 2 \\ &= \begin{cases} 0, & \text{if } m \equiv 0,3 \pmod 4 \\ 1, & \text{if } m \equiv 1,2 \pmod 4. \end{cases} \end{aligned}$$

Suppose 3 divides n. One checks that the non-zero elements of C are

$$\gamma_1 = \tfrac{n}{3}(011) \qquad \gamma_2 = \tfrac{n}{3}(101) \qquad \gamma_3 = \tfrac{n}{3}(110).$$

Now γ_2 and γ_3 are not in U since $B_2(\gamma_2, u_2) = B_2(\gamma_3, u_2) = 1$. But γ_1 is in U, in fact,

$$\gamma_1 = u_2 + \sum_{i \equiv 0,1 \pmod 3} u_i.$$

This also checks condition (8) of §2. For condition (9), take $\bar{z}_2 = z_2 + (C \cap U)$. $\square$

Now simply plug the values from (3.3)(2) and (3.3)(3) into the formulas of (2.5) and (2.6) to get:

Theorem 3.4. *(1) For $n = 2m+1$ odd, $n > 1$ and 3 not dividing n, we have*

$$F(n, \epsilon_1, \epsilon_2, \epsilon_3) = 2^{n-3} +$$

m	000	001	010	011	100	101	110	111
0	$3 \cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}	-2^{m-2}	$3 \cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}	-2^{m-2}
1	$-3 \cdot 2^{m-2}$	2^{m-2}	2^{m-2}	2^{m-2}	2^{m-2}	2^{m-2}	2^{m-2}	$-3 \cdot 2^{m-2}$
2	$-3 \cdot 2^{m-2}$	2^{m-2}	2^{m-2}	2^{m-2}	$-3 \cdot 2^{m-2}$	2^{m-2}	2^{m-2}	2^{m-2}
3	$3 \cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	$3 \cdot 2^{m-2}$

where the m is listed modulo 4.

(2) For $n = 2m+1$ odd, $n > 1$ and 3 dividing n, we have

$$F(n, \epsilon_1, \epsilon_2, \epsilon_3) = 2^{n-3} +$$

m	000	001	010	011	100	101	110	111
0	0	2^{m-1}	2^{m-1}	-2^{m}	0	2^{m-1}	-2^{m}	2^{m-1}
1	0	-2^{m-1}	-2^{m-1}	2^{m}	-2^{m-1}	2^{m}	-2^{m-1}	0
2	0	-2^{m-1}	-2^{m-1}	2^{m}	0	-2^{m-1}	2^{m}	-2^{m-1}
3	0	2^{m-1}	2^{m-1}	-2^{m}	2^{m-1}	-2^{m}	2^{m-1}	0

where again the m is listed modulo 4.

Note that our proof is only valid for $n \geq 7$. The above table however is also valid for $n = 3, 5$, which must be checked directly.

4. Irreducible polynomials.

We get formulas for the number of irreducible polynomials over $GF(2)$ with the first three coefficients prescribed, $P(n, \epsilon_1, \epsilon_2, \epsilon_3)$, from the inversion formulas of [8, Theorem 2]. For n odd these simplify slightly to:

$$P(n, 0, \epsilon_2, \epsilon_3) = \frac{1}{n} \sum_{d|n} \mu(d) F(n/d, 0, \epsilon_2, \epsilon_3)$$

$$P(n, 1, \epsilon_2, \epsilon_3) = \frac{1}{n} \sum_{\substack{d|n \\ d \equiv 1}} \mu(d) F(n/d, 1, \epsilon_2, \epsilon_3) + \frac{1}{n} \sum_{\substack{d|n \\ d \equiv 3}} \mu(d) F(n/d, 1, 1+\epsilon_2, 1+\epsilon_3).$$

The congruences here are modulo 4. The tables in (3.4) for F do not include the case $n = 1$ but these may arise in these inversion formulas. The values are $F(1,0,0,0) = F(1,1,0,0) = 1$ and the six others are 0.

As an example, suppose $n = 9$. The formulas become:

$$P(9,0,\epsilon_2,\epsilon_3) = \tfrac{1}{9}\left(F(9,0,\epsilon_2,\epsilon_3) - F(3,0,\epsilon_2,\epsilon_3)\right)$$
$$P(9,1,\epsilon_2,\epsilon_3) = \tfrac{1}{9}(F(9,1,\epsilon_2,\epsilon_3) - F(3,1,1+\epsilon_2,1+\epsilon_3)).$$

From the tables in (3.4) we get:

$$\begin{array}{ll} P(9,0,0,0) = 7 & P(9,1,0,0) = 7 \\ P(9,0,0,1) = 8 & P(9,1,0,1) = 8 \\ P(9,0,1,0) = 8 & P(9,1,1,0) = 5 \\ P(9,0,1,1) = 5 & P(9,1,1,1) = 8. \end{array}$$

These may be verified from Table C in [6, p. 553].

References

1. L. Carlitz, *A theorem of Dickson on irreducible polynomials*, Proc. Amer. Math. Soc. **3** (1952), 693–700.
2. K. Cattell, C. R. Miers, F. Ruskey, M. Serra and J. Sawada, *The number of irreducible polynomials over GF(2) with given trace and subtrace*, Preprint.
3. D. Jungnickel, *Finite fields : structure and arithmetics.*, Bibliographisches Institut, Mannheim, 1993.
4. M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The Book of Involutions*, Amer. Math. Soc. Colloquium Publications, vol. 44, Amer. Math. Soc., Providence, RI, 1998.
5. E. N. Kuz'min, *On a class of irreducible polynomials over a finite field*, Dokl. Akad. Nauk SSSr **313** (1990), no. 3, 552–555 (Russian); English translation in Soviet Math. Dokl. **42** (1991), no. 1, 45–48.
6. R. Lidl and H. Niederreiter, *Finite Fields (second edition)*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
7. W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren Math. Wiss., vol. 270, Springer-Verlag, New York/Heidelberg/Berlin, 1985.
8. J. L. Yucas and G. L. Mullen, *Irreducible polynomials over GF(2) with prescribed coefficients*, Preprint.

Carbondale, IL 62901
E-mail address: rfitzg@math.siu.edu, jyucas@math.siu.edu