Aspects of The Ring of Invariants of the Orthogonal Group over Finite Fields in Odd Characteristic

by

SUE BARNES

A thesis submitted to the
Faculty of Information and Mathematical Sciences
at the University of Glasgow
for the degree of
Doctor of Philosophy

2008

© S Barnes 2008

Abstract

Let V be a non-zero finite dimensional vector space over a finite field $\mathbb{F}_q$ of odd characteristic.

Fixing a non-singular quadratic form ξ_0 in $S^2(V^*)$, the symmetric square of the dual of V we are concerned with the Orthogonal group $O(\xi_0)$, the subgroup of the General Linear Group GL(V) that fixes ξ_0 and with invariants of this group.

We have the Dickson Invariants which being invariants of the General Linear Group are then invariants of $O(\xi_0)$. Considering the $O(\xi_0)$ orbits of the dual vector space V^* we generate the Chern Orbit polynomials, the coefficients of which, the Chern Orbit Classes, are also invariants of the Orthogonal group. The invariants $\xi_1, \xi_2, \ldots$ are be generated from ξ_0 by applying the action of the Steenrod Algebra to $S^2(V^*)$ which being natural takes invariants to invariants. Our aim is to discover further invariants from these known invariants with the intention of establishing a set of generators for the the Ring of invariants of the Orthogonal Group.

In particular we calculate invariants of $O(\xi_0)$ when the dimension of the vector space is 4 the finite field is $\mathbb{F}_3$ and the quadratic form is $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and we are able to establish an explicit presentation of $O(\xi_0)$ in this case.

Acknowledgements

There are a many people without whose very different support this thesis would have not been completed and I would like to thank them all. Firstly, I would like to thank my supervisor Peter Kropholler for his expertise in and enthusiasm for Invariant theory; for providing me with the motivation for this study and for his belief in my ability to produce some worthwhile research. Secondly I must say a special thank you to my second supervisor Kenny Brown for his calm, quiet, thorough and patient help when I needed it most.

Most importantly however, I could not have imagined completing on this research without the unwavering belief that my husband, Peter Barnes, has maintained in me throughout a very long four years. He has continually supported me in my every whim and put up with my foibles and quirks with incredible patience and I owe him a great debt of gratitude.

I have been encouraged along the way as, in turn, each of my children; Tom, Joanna and Mark has chosen to follow me into the wonderful world of Mathematics. In addition I need to thank the rest of my family for their support; especially my mother, an outstanding if unsung intellectual.

I would like to thank the many staff and post grads in the Glasgow University Mathematics Department and in the Faculty of Information, Mathematics and Statistic who have offered an encouraging or understanding word at just the right moment and in particular, Chris Athorne, Sandra Pott and Ian Strachan for their support and a sympathetic ear when times got hard.

Lastly I thank my father Valentine Geoffrey, my inspiration to see it through to the bitter end.

Contents

Chapter 1

Bilinear and quadratic forms

In this chapter we review the theory of bilinear forms and quadratic forms. We present definitions of these in §1 together with the definitions of some particular bilinear forms and we consider the relationship between the different forms. In §2 we set the context for quadratic forms in defining the Symmetric Algebra on the dual of a vector space. We consider quadratic forms with respect to a given basis in §3 and establish the map that a given quadratic form defines between the vector space and its dual.

1.1 Bilinear forms and quadratic forms

Given a finite dimensional vector space V and an arbitrary field K we have the following definitions.

Definition 1.1. A *bilinear form* is a map $b : V \times V \longrightarrow K$ such that, $\forall\ u, v, w \in V$:

(i) $b(v, u + w) = b(v, u) + b(v, w)$,

(ii) $b(v + w, u) = b(v, u) + b(w, u)$ and

(iii) $b(\alpha v, u) = b(v, \alpha u) = \alpha b(v, u)$.

Definition 1.2. A *quadratic form* is a map $Q : V \longrightarrow K$ such that:

(i) $\forall\ v \in V,\ \alpha \in K, \quad Q(\alpha v) = \alpha^2 Q(v)$ and

(ii) the map

$$\begin{aligned} V \times V &\longrightarrow K \\ (u, v) &\longmapsto Q(u+v) - Q(u) - Q(v) \end{aligned}$$

is bilinear.

For example, if $b : V \times V \longrightarrow K$ is a bilinear form then the function $Q : V \longrightarrow K$ defined by $Q(v) = b(v, v)$ is a quadratic form in the sense of our definition as:

(i) $Q(\alpha v) = b(\alpha v, \alpha v) = \alpha^2 b(v, v) = \alpha^2 Q(v)$ and

(ii)

$$\begin{aligned} Q(u+v) - Q(u) - Q(v) &= b(u+v, u+v) - b(u, u) - b(v, v) \\ &= b(u, u) + b(u, v) + b(v, u) + b(v, v) - b(u, u) - b(v, v) \\ &= b(u, v) + b(v, u) \end{aligned}$$

which is bilinear being the sum of bilinear forms.

If $Q(v)$ is a quadratic form we say that the bilinear form $b(u, v) = Q(u+v) - Q(u) - Q(v)$ is obtained by *polarizing* the quadratic form and that b is the *polarization* of Q for which we will use the notation $\mathcal{P}(Q)$.

When the characteristic of K is odd the quadratic form is uniquely determined by its polarization:

$$b(v, v) = Q(2v) - Q(v) - Q(v) = 4Q(v) - 2Q(v) = 2Q(v)$$

and hence

$$Q(v) = \frac{1}{2} b(v, v).$$

Since, in this thesis, we are concerned with the odd characteristic case only we will incorporate the factor of $\frac{1}{2}$ in our definition of polarization.

Definition 1.3. The polarization, $\mathcal{P}(Q)$, of the quadratic form $Q(v)$ is taken to be the bilinear form b such that

$$b(u, v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v)).$$

Then

$$Q(v) = b(v, v).$$

Definition 1.4. A bilinear form b is *symmetric* if $\forall\, u, v \in V \quad b(u, v) = b(v, u)$

We see that the polarization of a quadratic form is a symmetric bilinear form and so when the characteristic of the field is odd, there is a bijection between symmetric bilinear forms and quadratic forms.

Definition 1.5. A bilinear form b is *reflexive* if $\quad b(u, v) = 0 \Leftrightarrow b(v, u) = 0.$

Definition 1.6. A bilinear form b is *non-degenerate* if

$$\text{for each } v \in V \text{ with } v \neq 0 \quad \exists u, w \in V \mid b(v, u) \neq 0 \text{ and } b(w, v) \neq 0.$$

Definition 1.7. The *radical* (or *kernel*) of a bilinear form b, $\operatorname{rad} b$, is the set of vectors *orthogonal* with every other vector in V where vectors $v, u \in V$ are orthogonal if $b(v, u) = 0$ and $b(u, v) = 0$.

Hence, a bilinear form is non-degenerate if its radical is zero (or its kernel is trivial).

Definition 1.8. If $Q : V \longrightarrow K$ is a quadratic form then the *radical* (or kernel) of Q is

$$\operatorname{rad} Q = \{v \in V \mid v \in \operatorname{rad} \mathcal{P}(Q) \text{ and } Q(v) = 0\}.$$

The radical of Q which is contained in the radical of $\mathcal{P}(Q)$ is a subspace of V.

Definition 1.9. Q is *non-singular* iff $\operatorname{rad} Q = 0$.

Lemma 1.10. *In odd characteristic a quadratic form is non-singular (non-degenerate) if and only if its associated bilinear form is non-degenerate.*

Proof. (i) Let Q be a quadratic form such that $b = \mathcal{P}(Q)$ is non degenerate.

Then $\operatorname{rad} \mathcal{P}(Q) = 0$. But $\operatorname{rad} Q \subseteq \operatorname{rad} \mathcal{P}(Q)$ and so $\operatorname{rad} Q = 0$.

Hence Q is non singular.

(ii) Let Q be a quadratic form such that $b = \mathcal{P}(Q)$ is degenerate.

Then there exists $0 \neq u \in V$ such that $u \in \operatorname{rad} b$ and it follows that

$$\forall v \in V \quad b(u, v) = b(v, u) = 0.$$

Now $Q(u) = b(u, u)$ and $b(u, u) = 0$ so $u \in \operatorname{rad} Q$. Hence Q is singular.

□

Definition 1.11. A bilinear form b is *alternating* if $\quad b(v,v) = 0 \; \forall v \in V$.

Lemma 1.12 ([5], Theorem 6.1.3)**.** *A non-degenerate reflexive bilinear form is either symmetric or alternating.*

Proof. By commutativity of multiplication in K we have that

$$b(u,v)b(u,w) - b(u,w)b(u,v) = 0$$

and using the axioms of bilinearity it follows that

$$b[u, b(u,v)w] - b[u, b(u,w)v] \; = \; b[u, b(u,v)w - b(u,w)v] \; = 0.$$

Then as the bilinear form is reflexive

$$b[b(u,v)w - b(u,w)v, u] \; = 0$$

and so by bilinearity once more

$$b(u,v)b(w,u) - b(u,w)b(v,u) = 0. \tag{1.1}$$

Now say that a vector $u \in V$ is *good* if $b(u,v) = b(v,u) \neq 0$ for some $v \in V$, that u is *symmetric* if $b(u,w) = b(w,u)$ for all $w \in V$ and that u is *alternating* if $b(u,u) = 0$. By Equation 1.1 we see that if u is good then u is symmetric and as b is non-degenerate the converse is also true. From the definition of good we have that if u is good then so is v.

Now as b is non singular, for each element $u_i \in V$ there exists $v_i \in V$ such that $b(u_i, v_i) \neq 0$. We consider this statement for any two elements u_1, u_2 and deduce that for v equal to at least one of $v_1, v_2, v_1 + v_2$ both $b(u_1, v) \neq 0$ and $b(u_2, v) \neq 0$.

Let u_i be good then it follows, for some $u_j \neq u_i$ and some v_i, that $b(u_i, v_i) \neq 0$ and $b(u_j, v_i) \neq 0$. Then as u_i is symmetric

$$b(u_i, v_i) = b(v_i, u_i) \neq 0.$$

Thus v_i is good and so symmetric.

Hence

$$b(v_i, u_j) = b(u_j, v_i) \neq 0$$

and so u_j is good. Repeating this argument we see that if one vector in V is good then all are good. Hence b is symmetric.

If we let $w = u$ in Equation 1.1 we have

$$b(u,v)b(u,u) - b(u,u)b(v,u) = b(u,u)b(u,v) - b(u,u)b(v,u) = 0, \quad \forall u, v \in V.$$

Thus

$$b(u,u)(b(u,v) - b(v,u)) = 0, \quad \forall u, v \in V.$$

Thus for each u either $b(u,u) = 0$ or $b(u,v) - b(v,u) = 0$ for all v in V. If $b(u,v) - b(v,u) = 0 \; \forall v \in V$ then u is symmetric and so good and so all $v \in V$ are good. Thus b is symmetric. If no u is good then $b(u,u) = 0 \; \forall u \in V$ and so b is alternating. □

1.2 The Dual vector space, and the Symmetric algebra on the dual of V

Definition 1.13. V^* is the *dual* of the vector space V, being the space of linear maps from V to K.

Lemma 1.14. *If dim $V < \infty$ then V and V^* have the same dimension and $V \cong V^*$.*

Proof. Let the dimension of V be n and a basis for V be $e_1, e_2, \ldots e_n$. Then there exists a dual basis $x_1, x_2, \ldots, x_n$ such that $x_i(e_j) = \delta_{ij}$ where δ_{ij} is the *Kronecker delta*. That is $\delta_{ij} = 1$ if $i = j$ and zero otherwise. The result follows. □

Let V and W be vector spaces over a field K. Given a map $\alpha : V \longrightarrow W$ we have the dual map $\alpha^* : W^* \longrightarrow V^*$. We see that * is a contravariant functor.

The map α^* is defined so that

$$\alpha^*(\zeta)(v) = \zeta(\alpha(v)) \tag{1.2}$$

for each map $\zeta : W \longrightarrow K \; \in W^*$ and each vector $v \in V$. Then $\alpha^*(\zeta)$ is a map in V^* such that $\alpha^*(\zeta) : V \longrightarrow K$.

Now let the dimension of V be n and that of W be m and let $e_1, e_2, \ldots, e_n$ be a basis of V and $f_1, f_2, \ldots, f_m$ be a basis of W.

If

$$\alpha(e_i) = \sum_{j=1}^{m} a_{ji} f_j$$

for each $i = 1 \ldots n$ then we have the $m \times n$ matrix $A = (a_{ij})$ associated with the map α.

Lemma 1.15. *The matrix associated with the dual map α^* is the transpose of the matrix associated with the map α.*

Proof. Each basis $e_1, e_2, \ldots, e_n$ of V gives rise to a dual basis $x_1, x_2, \ldots, x_n$ of V^* where $x_i(e_j) = \delta_{ij}$ the Kronecker delta. Similarly each basis $f_1, f_2, \ldots, f_n$ of W gives rise to a dual basis $y_1, y_2, \ldots, y_n$ of W^*.

If

$$\alpha^*(y_i) = \sum_{j=1}^{n} \lambda_{ji} x_j$$

then the $n \times m$ matrix $B = (\lambda_{ij})$ is the matrix associated to the map α^*.

Evaluating on e_k we have

$$\begin{aligned} E_{e_k}(\alpha^*(y_i)) &= E_{e_k}\left(\sum_{j=1}^{n} \lambda_{ji} x_j\right) = \sum_{j=1}^{n} \lambda_{ji} x_j \quad (e_k) \\ &= \sum_{j=1}^{n} \lambda_{ji}\, x_j(e_k) = \sum_{j=1}^{n} \lambda_{ji} \delta_{jk} = \lambda_{ki}. \end{aligned}$$

However,

$$\begin{aligned} E_{e_k}(\alpha^*(y_i)) &= \alpha^*(y_i)(e_k) = y_i(\alpha(e_k)) = y_i\left(\sum_{j=1}^{m} a_{jk} f_j\right) \\ &= \sum_{j=1}^{m} a_{jk}\, y_i(f_j) = \sum_{j=1}^{m} a_{jk} \delta_{ij} = a_{ik}. \end{aligned}$$

Hence $\lambda_{ki} = a_{ik}$ and so $B = A^T$. □

Now we let $W = V^*$ the dual of V. Then

$$\alpha^* : V^{**} \longrightarrow V^*$$

where V^{**} is the double dual of V. If V is of finite dimension then $\dim V = \dim V^* = \dim V^{**}$ and we can identify V^{**} with V and so we have $\alpha^* : V \longrightarrow V^*$. For proofs see [10].

Definition 1.16. Given a bilinear form b we define a pair of maps $\acute{b}$ and $\grave{b}$ from V to its dual such that:

$$\begin{aligned} \acute{b} : V &\longrightarrow V^* \\ u &\longmapsto \acute{b}(u) = b(u, \cdot\,) \end{aligned}$$

$$\text{where} \qquad \begin{aligned} \acute{b}(u) : V &\longrightarrow K \\ v &\longmapsto b(u, v) \end{aligned}$$

and

$$\begin{aligned} \grave{b} : V &\longrightarrow V^* \\ u &\longmapsto \grave{b}(u) = b(\cdot\,, u) \end{aligned}$$

$$\text{where} \qquad \begin{aligned} \grave{b}(u) : V &\longrightarrow K \\ v &\longmapsto b(v, u) \end{aligned}$$

Lemma 1.17. *The bilinear form b is non-degenerate if and only if the map*

$$\begin{aligned} \acute{b} : V &\longrightarrow V^* \\ u &\longrightarrow b(u, \cdot\,) \end{aligned}$$

is injective and so bijective.

Proof. By Definition 1.7 a bilinear form b is non-degenerate if $\operatorname{rad}(b)$ is zero, that is if the only vector $v \in V$ for which $b(u, v) = b(v, u) = 0, ; \forall u \in V$ is the zero vector. Thus in this case the kernel of the map $\acute{b}$ is trivial and the map is injective.

If the form is degenerate bilinear form then $\operatorname{rad}(b)$ is non-zero and so there exists a vector $v \in V$ such that $b(u, v) = b(v, u) = 0$ for all $u \in V$ and thus the kernel of the map $\acute{b}$ is non trivial. Thus the map is not injective. □

Lemma 1.18. *The map $\grave{b}$ is the dual (or transpose) of $\acute{b}$ and vice versa. Thus the ranks of the maps $\acute{b}$ or $\grave{b}$ are equal.*

Proof. Given the maps $\acute{b}$ and $\grave{b}$ defined above we have the dual maps

$$(\acute{b})^* : V^{**} \longrightarrow V^* \quad \text{and} \quad (\grave{b})^* : V^{**} \longrightarrow V^*.$$

Now let $\hat{}$ be the map that identifies V^{**} with V so that $\hat{v} \in V^{**}$ identifies with $v \in V$.

Then we have

$$\begin{aligned} (\acute{b})^*(\hat{v})(w) &= \hat{v}(\acute{b}(w)) \quad \text{by Equation 1.2} \\ &= \acute{b}(w)(v) = b(w,v) \\ &= \grave{b}(v)(w) \end{aligned}$$

and

$$\begin{aligned} (\grave{b})^*(\hat{v})(w) &= \hat{v}(\grave{b}(w)) \quad \text{by Equation 1.2} \\ &= \grave{b}(w)(v) = b(v,w) \\ &= \acute{b}(v)(w) \end{aligned}$$

Thus we see that $(\acute{b})^* = \grave{b}$ and $(\grave{b})^* = \acute{b}$ and so the ranks of the maps $\acute{b}$ and $\grave{b}$ are equal.

□

Definition 1.19. It is clear that the maps $\acute{b}$ and $\grave{b}$ are identical if and only if b is symmetric. Thus we define the unique map $\hat{Q} = \acute{b} = \grave{b}$ determined by a given quadratic form Q such that

$$\begin{aligned} \hat{Q} : V &\longrightarrow V^* \\ u &\longrightarrow \hat{u} \end{aligned}$$

$$\begin{aligned} \text{where} \qquad \hat{u} : V &\longrightarrow K \\ v &\longmapsto b(u,v) = b(v,u). \end{aligned}$$

Definition 1.20. $S(V^*)$ is the *symmetric algebra* on the dual of V.

If V^* has basis $x_1, x_2, \ldots, x_n$ then $S(V^*)$ is isomorphic to $K[x_1, x_2, \ldots, x_n]$, the polynomial ring in the indeterminates that form a basis of V^*.

$S(V^*)$ is a graded algebra and so can be decomposed into summands $S^i(V^*)$, the ith *symmetric power* of V. Each summand $S^i(V^*)$ is spanned by the monomials of vectors in V^* of degree i. Thus $S^2(V^*)$ is the *symmetric square* comprising homogeneous polynomials of degree 2, that is quadratic forms.

1.3 Quadratic forms in Component form

Now let V be n-dimensional vector space and let $\mathcal{E} = [e_1, e_2, \ldots, e_n]$ be a basis for V. We can then associate a matrix B with the bilinear form b where

$$B_{ij} = b(e_i, e_j) \quad i, j = 1, 2, \ldots, n.$$

If e_u and e_v represent the vectors u and v respectively with respect to the basis $\mathcal{E}$ then

$$b(u, v) = e_u^T \, B \, e_v$$

where the superscript X^T denotes the transpose of the matrix X.

Given another basis $\mathcal{E}' = [e'_1, e'_2, \ldots, e'_n]$ for V we have

$$\mathcal{E}' = \mathcal{E}S$$

where S is an $n \times n$ invertible matrix. Then the matrix representation of the bilinear form with respect to the basis $\mathcal{E}'$ is

$$B' = S^T \, B \, S.$$

The bilinear form b is symmetric if and only if the matrix B is a symmetric matrix.
Hence if b is the polarization of the quadratic form Q then the associated matrix B is symmetric and

$$Q(u) = e_u^T \, B \, e_u.$$

Lemma 1.21. *A quadratic form is singular if and only if the associated matrix B is a singular matrix.*

Proof. Let Q be a singular quadratic form. Then we have that b, the polarization of Q is degenerate. Then $\operatorname{rad} b \neq 0$, that is there exists a non-zero vector $v \in V$ such that $b(u,v) = b(v,u) = 0 \quad \forall\, u \in V$. Hence $e_u^T\, B\, e_v = 0$ and so B is singular.

If the associated matrix B is singular then there exists some non zero $v \in V$ such that $Be_v = 0$ and so $b(u,v) = e_u^T\, B\, e_v = 0, \ \forall\, u \in V$ and so b is degenerate and so Q is singular. □

Lemma 1.22. *A quadratic form Q is singular if and only if there is a change of coordinate system that reduces the form to one in fewer variables.*

Proof. Let Q be a singular quadratic form. Then given the basis $\mathcal{E} = [e_1, e_2, \ldots, e_n]$ of V the associated $n \times n$ matrix B with respect to the basis $\mathcal{E}$ is singular. Hence there exists a matrix S such that the matrix $B' = S^T\, B\, S$ is a diagonal matrix with fewer than n non zero entries. □

Given a basis $x_1, x_2, \ldots x_n$ for V^* we have the general quadratic form

$$Q = \sum_{i,j=1}^{n} \beta_{ij} x_i x_j.$$

We can choose the β_{ij}'s so that each $\beta_{ij} = \beta_{ji}$. Thus we have a symmetric matrix B with $B_{ij} = \beta_{ij}$ such that

$$Q(x) = x^T B x$$

where x is the column vector with components $x_1, x_2, \ldots, x_n$ and x^T is the transpose of x.

The matrix B is also the matrix associated with the bilinear form b that is the polarization of Q so that

$$b(u,v) = u^T B v.$$

Given a general quadratic form in component form we can determine explicitly the vector in the dual corresponding to a given vector in V with reference to Lemma 1.19.

Lemma 1.23. *Let $e_1, e_2, \ldots, e_n$ be a basis of V and $x_1, x_2, \ldots, x_n$ be the dual basis of V^*. Take a vector*

$$u = \sum_{i=1}^{n} \lambda_i e_i \in V$$

and the quadratic form

$$Q = \sum_{i,j=1}^{n} \beta_{ij}\, x_i x_j.$$

Then the map $\hat{Q}$ of Definition 1.19 determined by the quadratic form Q is such that

$$\begin{array}{rcl} \hat{Q} : V & \longrightarrow & V^* \\ u & \longrightarrow & \hat{u} \end{array}$$

where

$$\hat{u} = \sum_{i=1}^{n} a_i x_i \quad \textit{with} \quad a_i = \sum_{i=1}^{n} \beta_{ik}\lambda_i.$$

Proof. Let

$$\hat{u} = \sum_{i=1}^{n} a_i x_i.$$

Then for each $k = 1 \ldots n$,

$$b(u, e_k) = \hat{u}(e_k) = a_k.$$

Now we have

$$\begin{aligned} b(u,e_k) &= \frac{1}{2}\left[Q(u+e_k) - Q(u) - Q(e_k)\right] \\ &= \frac{1}{2}\left[\beta_{kk}(\lambda_k+1)^2 + \sum_{k\neq i=1}^{n} \beta_{ik}\lambda_i(\lambda_k+1)) + \sum_{k\neq j=1}^{n} \beta_{kj}(\lambda_k+1)\lambda_j) + \sum_{i,j\neq k,\, i,j=1}^{n} \beta_{ij}\,\lambda_i\lambda_j\right] \\ &\quad -\frac{1}{2}\left[\sum_{i,j=1}^{n} \beta_{ij}\,\lambda_i\lambda_j + \beta_{kk}\right] \\ &= \frac{1}{2}\left[2\beta_{kk}\lambda_k + \sum_{k\neq i=1}^{n} \beta_{ik}\lambda_i + \sum_{k\neq j=1}^{n} \beta_{kj}\lambda_j\right] \\ &= \sum_{i=1}^{n} \beta_{ik}\lambda_i \qquad \text{as } \beta_{ij} = \beta_{ji}. \end{aligned}$$

Hence we have

$$\hat{u} = \sum_{i=1}^{n} a_i x_i \quad \text{where} \quad a_i = \sum_{i=1}^{n} a_{ik}\lambda_i.$$

□

Chapter 2

The Orthogonal group over fields of odd characteristic

In this chapter we continue to review the theory leading toward the definition of the Orthogonal groups over finite fields restricting our attention in this and future chapters to finite fields of odd characteristic. §1 is started by defining a finite field and then we establish some properties of finite fields. These properties are required in §2 for the discussion of the equivalence of quadratic forms where we also define the General Linear Group. Then in §3 we consider the classification of quadratic spaces and in §4 we define the Orthogonal groups, subgroups of the General Linear group, and state their number and order.

2.1 Some properties of Finite fields

Definition 2.1. A *finite field* is a field with a finite number of elements. We denote by $\mathbb{F}_q$ the finite field with q elements.

Definition 2.2. The *characteristic* of a finite field is the smallest number of times that the multiplicative identity must be added to produce the additive identity.

Lemma 2.3 ([14] Theorem 2.2)**.** *Let $\mathbb{F}_q$ be a finite field then $q = p^r$ where the prime p is the characteristic of $\mathbb{F}_q$ and r is the degree of $\mathbb{F}_q$ over its prime subfield $\mathbb{F}_p$.*

Lemma 2.4 ([14] Theorem 2.5)**.** *For every prime p and every positive integer r there exists a finite field with p^r elements. Any finite field with $q = p^r$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.*

We now present some properties of finite fields which will be used in later sections.

We define $\mathbb{F}_q^*$ to be the elements of the multiplicative group of the finite field $\mathbb{F}_q$. That is

$$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}.$$

Lemma 2.5 ([2] Theorem 9.4)**.** *If $q \equiv 1 (\bmod 4)$ then -1 is a square and if $q \equiv 3 (\bmod 4)$ then -1 is a non-square.*

Lemma 2.6 ([22] Corollary 20.9)**.** *The multiplicative group of a finite field is cyclic.*

Lemma 2.7. *If $\alpha \in \mathbb{F}_q$ then $\alpha^q = \alpha$.*

Proof. Firstly $0^q = 0$. As the elements of $\mathbb{F}_q^*$ form the multiplicative group of the finite field $\mathbb{F}_q$ so $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$ as the order of the group is $q - 1$. Thus $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q^*$. □

Lemma 2.8. *The product of all the non zero elements of a finite field is -1.*

Proof. The multiplicative group $\mathbb{F}_q^*$ is cyclic by Lemma 2.6 and so there exists an element $\beta \in \mathbb{F}_q^*$ that generates the group so that for each $\alpha \in \mathbb{F}_q^*$, $\alpha = \beta^i$ for some $1 \leq i \leq q-1$. That is the group $\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^{q-1}\}$. It then follows that the product of the elements in $\mathbb{F}_q^*$ is

$$\begin{aligned} \prod_{i=1}^{q-1} \beta^i &= \beta^{1+2+\cdots+q-1} \\ &= (\beta^q)^{\frac{q-1}{2}} \\ &= \beta^{\frac{q-1}{2}} \quad \text{by Lemma 2.7.} \end{aligned}$$

As $\beta^{q-1} = 1$ by Lemma 2.7 and as β is a generator of the group it follows that $\beta^{\frac{q-1}{2}} = -1$.

Thus the product of the elements of $\mathbb{F}_q^*$ is -1 as required. □

Lemma 2.9. *Every non-square element of $\mathbb{F}_q$ can be written as the product of any given non-square with a square.*

Proof. Let ν_i be any non-square and ν a given non square in $\mathbb{F}_q$. Then we require that $\nu_i = \alpha^2\nu$ for some α in $\mathbb{F}_q$. We must have $\nu_i = \beta\nu$ for some $\beta \in \mathbb{F}_q$ and β must be a square by the following argument. There are $\frac{q-1}{2}$ squares and $\frac{q-1}{2}$ non-squares in $\mathbb{F}_q^*$ the set of non zero elements of $\mathbb{F}_q$ that form a group under multiplication. We have that $\alpha_i^2 \times \alpha_j^2 = (\alpha_i\alpha_j)^2$ thus the product of two squares is a square. It follows that the product of a square with a non-square must be a non-square by a counting argument and thus the product of a non-square with a non-square must be a square. Thus β must be a square. □

Lemma 2.10 ([12], Lemma 5.6)**.** *Every non-square element of $\mathbb{F}_q$ can be written as the sum of two squares in $\mathbb{F}_q$.*

Definition 2.11. Working with the vector space V over the finite field $\mathbb{F}_q$ where $p = q^r$ for prime p we define the *Frobenius map*, $\Phi : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V]$ induced by the map on linear forms $\phi : x \mapsto x^p$.

Lemma 2.12. *The Frobenius map, Φ defined in Lemma 2.11 is a automorphism.*

Proof. It is easily seen that, $\forall\, x, y \in V$,

$\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y)$ as the characteristic of the field is p,

$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$ and

$\Phi(0) = 0^p = 0$ and $\Phi(1) = 1^p = 1$.

Thus Φ is an automorphism. □

Lemma 2.13. *The map*

$$\begin{aligned} \Phi' : \mathbb{F}_q[V] &\longrightarrow \mathbb{F}_q[V] \\ x &\longmapsto x^q \end{aligned}$$

where $q = p^r$ for prime p, is an automorphism.

Proof. Again it is easily seen that, $\forall\, x, y \in V$,

$\Phi'(xy) = (xy)^q = x^q y^q = \Phi(x)\Phi(y)$ and

$\Phi'(0) = 0^q = 0$ and $\Phi(1) = 1^q = 1$.

Now

$$\begin{aligned}
\Phi'(x+y) &= (x+y)^q = (x+y)^{p^r} \\
&= ((x+y)^p)^{p^{r-1}} = ((x^p + y^p))^{p^{r-1}} \quad \text{by Lemma 2.12} \\
&= ((x^p + y^p)^p)^{p^{r-2}} = ((x^{p^2} + y^{p^2} p)^{p^{r-2}} \quad \text{similarly} \\
&= \ldots \\
&= (x^{p^{r-1}} + y^{p^{r-1}})^p = x^{p^r} + y^{p^r} \quad \text{similarly} \\
&= x^q + y^q = \Phi'(x) + \Phi'(y).
\end{aligned}$$

Thus Φ' is an automorphism. □

2.2 Equivalence of quadratic forms.

Let V be an n dimensional vector space over $\mathbb{F}_q$ and let Q be a non-singular quadratic form in n variables over $\mathbb{F}_q$, with q odd.

Definition 2.14. The *General Linear Group* $GL(V)$ is the group of all the automorphisms of V.

If V is an n dimensional vector space over K then $GL(V)$ is isomorphic to the group of invertible n by n matrices over K denoted $GL_n(K)$. When $K = \mathbb{F}_q$ we denote $GL_n(\mathbb{F}_q)$ by $GL(n, q)$.

We take the action of $GL(V)$ on V to be a left action and the induced action on V^* to be a right action and write for $g \in GL(V)$, $v \in V$ and $x \in V^*$

$$\begin{array}{ccc} g : V \longrightarrow V & & g : V^* \longrightarrow V^* \\ v \longmapsto gv & \text{and} & x \longmapsto x^g. \end{array}$$

Furthermore $GL(V)$ acts on $S(V^*)$ and in particular on the set of quadratic forms on V^* on the right so that for $Q \in S^2(V^*)$

$$\begin{array}{rccc} g : & S^2(V^*) & \longrightarrow & S^2(V^*) \\ & Q & \longmapsto & Q^g \end{array}$$

If $v_1, v_2, \ldots, v_n$ is a basis for V and $x_1, x_2, \ldots, x_n$ a basis for V^* and if $g \in GL(V)$ is represented by a non-singular n by n matrix M and the non-singular quadratic form Q has an associated non-singular n by n matrix B such that $Q(x) = x^T Bx$.

Then

$$Q(x^g) = (x^g)^T B(x^g) = Mx^T BMx = x^T(M^T BM)x = x^T(Q^g)x = Q^g(x).$$

We consider forms Q_1 and Q_2 to be equivalent ($Q_1 \sim Q_2$) if Q_2 can be obtained from Q_1 by means of a change of coordinate system. That is

$$Q_1 \sim Q_2 \Leftrightarrow Q_2 = Q_1^g.$$

We establish below the equivalences between quadratic forms. First we establish some basic equivalences of forms in 2 and 4 variables.

Lemma 2.15. *(i) The form $x_1^2 + x_2^2 \sim x_1x_2$ when $q \equiv 1 \bmod 4$ and is irreducible when $q \equiv 3 \bmod 4$.*

(ii) If ν is a non-square in $\mathbb{F}_q^*$ then form $x_1^2 + \nu x_2^2 \sim x_1x_2$ when $q \equiv 3 \bmod 4$ and is irreducible when $q \equiv 1 \bmod 4$.

Proof. Firstly if $q \equiv 1 \bmod 4$ then -1 is a square and so $-\nu$, being the product of a non-square with a square, is a non-square as shown in the proof of Lemma 2.5 (ii). However if $q \equiv 3 \bmod 4$ then -1 is a non-square and so, similarly, $-\nu$, being the product of two non-squares, is a square.

If σ is a square in $\mathbb{F}_q^*$ then $x_1^2 - \sigma x_2^2 = (x_1 + \alpha x_2)(x_1 - \alpha x_2)$ for some $\alpha \in \mathbb{F}_q \setminus 0$ and so

$$x_1^2 - \sigma x_2^2 \sim x_1x_2.$$

The form $x_1^2 - \nu x_2^2$ is irreducible.

Now

(i) as $x_1^2 + x_2^2 = x_1^2 - (-1)x_2^2$ if $q \equiv 1 \bmod 4$ then $x_1^2 + x_2^2 \sim x_1x_2$ and if $q \equiv 3 \bmod 4$ then $x_1^2 + x_2^2$ is irreducible,

(ii) as $x_1^2 + \nu x_2^2 = x_1^2 - (-\nu)x_2^2$ if $q \equiv 3 \bmod 4$ then $x_1^2 + \nu x_2^2 \sim x_1x_2$ and if $q \equiv 1 \bmod 4$ then $x_1^2 + \nu x_2^2$ is irreducible for a non-square $\nu \in \mathbb{F}_q^*$.

□

Lemma 2.16. *For any non-square $\nu \in \mathbb{F}_q$ the form $\nu(x_1^2 + x_2^2)$ is equivalent to the form $x_1^2 + x_2^2$.*

Proof. We have that each non-square $\nu = \alpha^2 + \beta^2$ for some $\alpha, \beta \in \mathbb{F}_q$ by Lemma 2.10.

Thus

$$\begin{aligned} \nu(x_1^2 + x_2^2) &= (\alpha^2 + \beta^2)(x_1^2 + x_2^2) \\ &= (\alpha x_1 + \beta x_2)^2 + (\beta x_1 - \alpha x_2)^2 \\ &\sim x_1^2 + x_2^2. \end{aligned}$$

□

Lemma 2.17. *The form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is equivalent to the form $x_1x_2 + x_3x_4$*

Proof. If $q \equiv 1 \pmod 4$ the result follows from Lemma 2.15.

If $q \equiv 3 \pmod 4$ then -1 is a non-square. Hence by Lemma 2.16 we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &\sim x_1^2 + x_2^2 + (-1)(x_3^2 + x_4^2) = x_1^2 + x_2^2 - x_3^2 - x_4^2 \\ &= (x_1 - x_3)(x_1 + x_3) + (x_2 - x_4)(x_2 + x_4) \\ &\sim x_1x_2 + x_3x_4. \end{aligned}$$

□

Lemma 2.18. *A non singular quadratic form is equivalent to a diagonal quadratic form. That is*

$$Q \sim \sum_{i=1}^{n} \alpha_i x_i^2 \quad \text{for } \alpha_i \in \mathbb{F}_q \text{ and some } \alpha_i \neq 0.$$

Furthermore, in the above form we can have

- either $\alpha_1 = 1$ or $\alpha_1 = \nu$ and
- $\alpha_i = 1, \quad i = 2 \ldots n$

where ν is a non-square in $\mathbb{F}_q^*$.

Hence we have that a quadratic form is equivalent to one of

$$Q_s = \sum_{i=1}^{n} x_i^2 \quad \text{or} \quad Q_n = \nu x_1^2 + \sum_{i=2}^{n} x_i^2$$

for some non-square $\nu \in \mathbb{F}_q^*$.

Proof. Let the quadratic form

$$Q = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j, \quad \alpha_{ij} \in \mathbb{F}_q \text{ and some } \alpha_{i,j} \neq 0.$$

We can assume that each $\alpha_{ij} = \alpha_{ji}$.

If the form Q has some $\alpha_{kk} \neq 0$ then the transformation

$$x_1 = y_k,\ x_k = y_1, \quad x_i = y_i \quad i = 2, \ldots, k-1, k+1, \ldots, n$$

gives that

$$Q \sim \sum_{i,j=1}^{n} \beta_{ij} x_i x_j \quad \text{for some} \quad \beta_{ij} \in \mathbb{F}_q \quad \text{with} \quad \beta_{11} \neq 0.$$

Alternatively if $\alpha_{kk} = 0$ for all $k = 1, \ldots, n$ then we must have some k_1, k_2 with $\alpha_{k_1 k_2} \neq 0$. Then the transformation

$$x_{k_2} = y_{k_1} + y_{k_2}, \quad x_i = y_i \quad i = 1, \ldots, k_2 - 1, k_2 + 1, \ldots, n$$

followed by the transformation

$$y_1 = z_{k_1},\ y_{k_1} = z_1, \quad y_i = z_i \quad i = 2, \ldots, k_1 - 1, k_1 + 1, \ldots, n$$

again gives that

$$Q \sim \sum_{i,j=1}^{n} \beta_{ij} x_i x_j \quad \text{for some} \quad \beta_{ij} \in \mathbb{F}_q \quad \text{with} \quad \beta_{11} \neq 0.$$

In either case the transformation

$$y_1 = x_1 + \sum_{i=2}^{n} \gamma_i x_i, \quad y_i = x_i, \quad i = 2 \ldots n \quad \text{where each} \quad \gamma_i = \frac{\beta_{1i}}{\beta_{11}}$$

gives that

$$Q \sim Q_1 = \alpha_1 x_1^2 + Q_1'(x_2, x_3, \ldots, x_n) \quad \text{for some } \alpha_1 \in \mathbb{F}_q^*.$$

Repeating the process gives

$$Q \sim \sum_{i=1}^{n} \alpha_i x_i^2 \quad \text{for some } \alpha_i \in \mathbb{F}_q^*.$$

For each α_i that is a square in $\mathbb{F}_q^*$ there exists a $\beta_i \in \mathbb{F}_q^*$ such that $\alpha_i x_i^2 = (\beta_i x_i)^2$. Choosing any non-square $\nu \in \mathbb{F}_q^*$ for each α_i that is a non square in $\mathbb{F}_q^*$ there exists a $\beta_i \in \mathbb{F}_q^*$ such that $\alpha_i x_i^2 = \nu(\beta x_i)^2$. Hence with some reordering the transformation $y_i = \beta_i x_i \quad i = 1 \ldots n$ gives that

$$Q \sim \sum_{i=1}^{m} x_i^2 + \nu \sum_{i=m+1}^{n} x_i^2 \quad \text{for some} \quad 0 \leq m \leq n.$$

Now utilizing Lemma 2.16 we see that

$$Q \sim \nu x_1^2 + \sum_{i=2}^{n} x_i^2$$

if exactly one of m and n is even and

$$Q \sim \sum_{i=1}^{n} x_i^2$$

otherwise.

Thus we have the equivalences as required.

□

We now wish to show that each quadratic form is equivalent to one of the forms $Q+$ or $Q-$ as defined below. These forms are used later in the classification of quadratic forms leading into the determination of the number of the orthogonal groups at the end of this chapter.

Definition 2.19. We denote by Q_+ and Q_- the quadratic forms as follows.

- When $n = 2s$

$$Q_+ = \sum_{i=1}^{s} x_{2i-1}x_{2i} \quad \text{and} \quad Q_- = f(x_1, x_2) + \sum_{i=2}^{s} x_{2i-1}x_{2i}$$

where $f(x_1, x_2)$ is an irreducible quadratic form for example $f(x_1, x_2) = x_1^2 - \nu x_2^2$ where ν is a non-square in $\mathbb{F}_q^*$.

- When $n = 2s + 1$

$$Q_+ = x_1^2 + \sum_{i=1}^{s} x_{2i}x_{2i+1} \quad \text{and} \quad Q_- = \nu x_1^2 + \sum_{i=1}^{s} x_{2i}x_{2i+1}$$

where ν is a non square in $\mathbb{F}_q^*$.

We now prove the equivalences between the forms Q_+, Q_- and the forms Q_s, Q_n defined in the statement of Lemma 2.18.

Lemma 2.20. *(i) For even $n = 2s$,*

$Q_s \sim Q_+$ *and* $Q_n \sim Q_-$ *when either* $q \equiv 1(\bmod 4)$ *or* $n \equiv 0(\bmod 4)$ *and*

$Q_s \sim Q_-$ *and* $Q_n \sim Q_+$ *when* $q \equiv 3(\bmod 4)$ *and* $n \equiv 2(\bmod 4)$.

(ii) For odd $n = 2s + 1$

$Q_s \sim Q_+$*and* $Q_n \sim Q_1$ *when either* $q \equiv 1(\bmod 4)$ *or* $n \equiv 1(\bmod 4)$.

$Q_s \sim Q_-$ *and* $Q_n \sim Q_+$ *when both* $q \equiv 3(\bmod 4)$ *and* $n \equiv 3(\bmod 4)$.

Proof. Let ν be a non-square in $\mathbb{F}_q^*$.

(i) Let $n = 2s$.

When $q \equiv 1 \bmod 4$

$$\begin{aligned} Q_s &= \sum_{i=1}^{2s} x_i^2 = \sum_{i=1}^{s} x_{2i-1}^2 + x_{2i}^2 \\ &\sim \sum_{i=1}^{s} x_{2i-1}x_{2i} \quad \text{by Lemma 2.15} \\ &= Q_+ \end{aligned}$$

and

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{2s} x_i^2 = \nu x_1^2 + x_2^2 + \sum_{i=2}^{s} x_{2i-1}^2 + x_{2i}^2 \\ &\sim (f(x_1, x_2) + \sum_{i=2}^{s} x_{2i-1}x_{2i} \quad \text{by Lemmas 2.15 and 2.17,} \end{aligned}$$

where $f(x_1, x_2) = x_2^2 + \nu x_1^2$ is irreducible and so $Q_n \sim Q_-$.

When $n \equiv 0 \bmod 4$ we can let let $n = 4s'$ so that $s = 2s'$. We can assume that $q \equiv 3 \bmod 4$ as the case for $q \equiv 1 \bmod 4$ has been covered above.

Now

$$\begin{aligned} Q_s &= \sum_{i=1}^{2s} x_i^2 = \sum_{i=1}^{s'} x_{4i-3}^2 + x_{4i-2}^2 + x_{4i-1}^2 + x_{4i}^2 \\ &\sim \sum_{i=1}^{s'} x_{4i-3}x_{4i-2} + x_{4i-1}x_{4i} \quad \text{by Lemma 2.17} \\ &= \sum_{i=1}^{2s'=s} x_{2i-1}x_{2i} = Q_+ \end{aligned}$$

and

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{2s} x_i^2 \\ &= \nu x_1^2 + x_2^2 + x_3^2 + x_4^2 + \sum_{i=2}^{s'} x_{4i-3}^2 + x_{4i-2}^2 + x_{4i-1}^2 + x_{4i}^2 \\ &\sim x_1 x_2 + f(x_3, x_4) + \sum_{i=2}^{s'} x_{4i-3}x_{4i-2} + x_{4i-1}x_{4i} \quad \text{by Lemmas 2.15 and 2.17} \\ &= f(x_1, x_2) + \sum_{i=2}^{2s'=s} x_{2i-1}x_{2i} = Q_-. \end{aligned}$$

When $q \equiv 3 \bmod 4$ and $n \equiv 2 \bmod 4$ we can let $n = 4s' + 2$ so that $s = 2s' + 1$. Then

$$\begin{aligned} Q_s &= \sum_{i=1}^{4s'+2} x_i^2 = x_1^2 + x_2^2 + \sum_{i=1}^{s'} x_{4i-1}^2 + x_{4i}^2 + x_{4i+1}^2 + x_{4i+2}^2 \\ &\sim f(x_1, x_2) + \sum_{i=1}^{s'} x_{4i-1}x_{4i} + x_{4i+1}x_{4i+2} \quad \text{by Lemmas 2.15 and 2.17} \\ &= f(x_1, x_2) + \sum_{i=2}^{2s'+1=s} x_{2i-1}x_{2i} = Q_- \end{aligned}$$

and

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{4s'+2} x_i^2 \\ &= \nu x_1^2 + x_2^2 + \sum_{i=2}^{s'} x_{4i-1}^2 + x_{4i}^2 + x_{4i+1}^2 + x_{4i+2}^2 \\ &\sim x_1 x_2 + \sum_{i=1}^{s'} x_{4i-1}x_{4i} + x_{4i+1}x_{4i+2} \quad \text{by Lemmas 2.15 and 2.17} \\ &= \sum_{i=1}^{2s'+1=2s} x_{2i-1}x_{2i} = Q_+. \end{aligned}$$

(ii) Let $n = 2s + 1$.

When $q \equiv 1 \bmod 4$

$$\begin{aligned} Q_s &= \sum_{i=1}^{2s+1} x_i^2 = x_1^2 + \sum_{i=1}^{s} x_{2i}^2 + x_{2i+1}^2 \\ &\sim x_1^2 + \sum_{i=1}^{s} x_{2i}x_{2i+1} \quad \text{by Lemma 2.15} \\ &= Q_+ \end{aligned}$$

and

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{2s+1} x_i^2 = \nu x_1^2 + \sum_{i=1}^{s} x_{2i}^2 + x_{2i+1}^2 \\ &\sim \nu x_1^2 + \sum_{i=1}^{s} x_{2i}x_{2i+1} \quad \text{by Lemma 2.15} \\ &= Q_-. \end{aligned}$$

If $n \equiv 1 \bmod 4$ we can let let $n = 4s' + 1$ so that $s = 2s'$. We can assume that $q \equiv 3 \bmod 4$ as the case for $q \equiv 1 \bmod 4$ has been covered above.

Then

$$\begin{aligned} Q_s &= \sum_{i=1}^{4s'+1} x_i^2 = x_1^2 + \sum_{i=1}^{s'} x_{4i-2}^2 + x_{4i-1}^2 + x_{4i}^2 + x_{4i+1}^2 \\ &\sim x_1^2 + \sum_{i=1}^{s'} x_{4i-2}x_{4i-1} + x_{4i}x_{4i+1} \quad \text{by Lemma 2.17} \\ &= x_1^2 + \sum_{i=1}^{2s'=s} x_{2i}x_{2i+1} = Q_+ \end{aligned}$$

and

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{2s} x_i^2 = \nu x_1^2 + \sum_{i=1}^{s'} x_{4i-2}^2 + x_{4i-1}^2 + x_{4i}^2 + x_{4i+1}^2 \\ &\sim \nu x_1^2 + \sum_{i=1}^{s'} x_{4i-3}x_{4i-2} + x_{4i-1}x_{4i} \quad \text{by Lemma 2.17} \\ &= \nu x_1^2 + \sum_{i=1}^{2s'=s} x_{2i-1}x_{2i} = Q_-. \end{aligned}$$

When $n \equiv 3 \bmod 4$ we can let $n = 4s' + 3$ so $s = 2s' + 1$. Now if $q \equiv 3 \bmod 4$

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &\sim x_1^2 + \nu(x_2^2 + x_3^2) \quad \text{by Lemma 2.16} \\ &= (x_1^2 + \nu x_2^2) + \nu x_3^2 \\ &\sim x_1 x_2 + \nu x_3 \quad \text{by Lemma 2.15} \\ &\sim \nu x_1^2 + x_2 x_3. \end{aligned}$$

Then

$$\begin{aligned} Q_s &= \sum_{i=1}^{4s'+3} x_i^2 = x_1^2 + x_2^2 + x_3 + \sum_{i=1}^{s'} x_{4i}^2 + x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 \\ &\sim \nu x_1^2 + x_2 x_3 + \sum_{i=1}^{s'} x_{4i} x_{4i+1} + x_{4i+2} x_{4i+3} \quad \text{by the argument above and Lemma 2.17} \\ &= \nu x_1^2 + \sum_{i=1}^{2s'+1=s} x_{2i} x_{2i+1} = Q_- \end{aligned}$$

and

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{4s'+3} x_i^2 = \nu x_1^2 + x_2^2 + x_3^2 + \sum_{i=1}^{s'} x_{4i}^2 + x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 \\ &\sim x_1 x_2 + x_3^2 + \sum_{i=1}^{s'} x_{4i} x_{4i+1} + x_{4i+2} x_{4i+3} \quad \text{by Lemmas 2.15 and 2.17} \\ &\sim x_1^2 + x_2 x_3 + \sum_{i=1}^{s'} x_{4i} x_{4i+1} + x_{4i+2} x_{4i+3} \\ &= x_1^2 + \sum_{i=1}^{2s'+1=s} x_{2i} x_{2i+1} = Q_+. \end{aligned}$$

Thus we have the equivalences as required. □

Lemma 2.21. *Each non singular quadratic form in n variables is equivalent to one of Q_+ or Q_-.*

Proof. This follows from Lemmas 2.18 and 2.20. □

Lemma 2.22. *For odd $n = 2s + 1$ the quadratic form Q_n is equivalent to a non-square multiple of the form Q_s. Thus every quadratic form is equivalent up to scalar multiplication.*

Proof. We have

$$\begin{aligned} Q_n &= \nu x_1^2 + \sum_{i=2}^{2s+1} x_i^2 = \nu x_1^2 + \sum_{i=1}^{s} x_i^2 + x_{i+1}^2 \\ &\sim \nu x_1^2 + \nu \sum_{i=1}^{s} x_i^2 + x_{i+1}^2 \quad \text{by Lemma 2.16} \\ &= \nu Q_s \end{aligned}$$

as required. □

Definition 2.23. We say that a quadratic form Q is of plus type if $Q \sim Q_+$ and of minus type if $Q \sim Q_-$.

2.3 Classification of quadratic spaces

Having established the equivalences of quadratic forms in the previous section we now present an informal geometric interpretation of these forms. A more detailed and formal presentation is given from the perspective of Projective geometry in [12] and also in [5].

Definition 2.24.

(i) A *quadratic space* is a vector space endowed with a non-degenerate quadratic form denoted V_Q.

(ii) An *anisotropic* space is one on which the form is non zero on all non zero vectors.

(iii) An *isotropic* space is one on which the form is zero on at least one non zero vector. A space is *totally isotropic* if the form is zero on all points.

(iv) The dimension ω of a maximal totally isotropic subspace of a quadratic space V is called the *Witt index* of V.

(v) A *hyperbolic line* is a space that is spanned by vectors u_1 and u_2 such that the form is zero on both u_1 and u_2 and equal to 1 on $u_1 + u_2$. (Projectively this space is a line.)

Lemma 2.25 ([5] Theorem 6.3.1)**.** *A quadratic space is the direct sum of a number of hyperbolic lines, r and an anisotropic space, U. The number r and the isomorphism type of U are invariants of V.*

This number, r, of hyperbolic lines is the polar rank of of the quadratic space. It can be seen that the polar rank is equal to the Witt index of the space. Peter Cameron in [5] Section 6.3 defines the anisotropic space, U, to be the *germ* of the space having rank δ and so we have

$$\delta + 2\omega = n.$$

When V is of odd dimension $n = 2s + 1$ each non singular quadratic form is equivalent up to scalar multiplication by Lemma 2.22 and thus with reference to Lemma 2.25 we see that the values of ω and δ are invariant.

If

$$Q = x_1^2 + \sum_{i=1}^{s} x_{2i}x_{2i+1}$$

it can be seen that the anisotropic subspace U of V_Q is spanned by the vector x_1 and thus is of rank 1. Each product $x_{2i}x_{2i+1}$ gives rise to a hyperbolic line spanned by the vectors x_{2i} and x_{2i+1} and so V_Q is the product of s such hyperbolic lines and the space U. Thus when $n = 2s + 1$ the quadratic space V_Q has anisotropic subspace of dimension $\delta = 1$ and Witt index $\omega = s$.

When the vector space is of dimension $n = 2s$ a quadratic form of plus type is equivalent to

$$Q_+ = \sum_{i=1}^{s} x_{2i-1}x_{2i}.$$

For such a form it can be seen that there is no anisotropic subspace. Again each product $x_{2i-1}x_{2i}$ gives rise to a hyperbolic line spanned by the vectors x_{2i-1} and x_{2i}. Thus in this case V_Q is the product s hyperbolic lines.

A space V of dimension $n = 2s$ endowed with the form $Q_- = f(x_1, x_2) + \sum_{i=2}^{s} x_{2i-1}x_{2i}$ where $f(x_1, x_2)$ is an irreducible form can be seen to have an anisotropic subspace of rank 2 spanned by the vectors x_1 and x_2 and to be the product of $s-1$ hyperbolic lines spanned by the pairs of vectors x_{2i-1} and x_{2i} for $i = 2, \ldots, s$.

Thus, with reference to Lemma 2.21 and Lemma 2.25 a quadratic space V_Q of even dimension has either $\delta = 0$ and Witt index $\omega = s$ when the quadratic form Q is of plus type has or $\delta = 2$ and Witt index $\omega = s - 1$ when the form of minus type.

2.4 The Orthogonal group

Definition 2.26. Let Q be a non-singular quadratic form and denote by $O(Q)$ the *Orthogonal Group* determined by Q:

$$O(Q) = \{g \in GL(V^*) \mid Q^g = Q\}$$

That is, $O(Q)$ is the subset of $GL(V)$ under which Q is invariant.

Lemma 2.27. *When n is odd, say $n = 2s+1$ there is only one orthogonal group up to isomorphism which we denote $O(n,q)$ so that, in this case, $O(Q) \cong O(n,q)$ for all quadratic forms Q.*

When n is even say $n = 2s$ there are two orthogonal groups up to isomorphism denoted $O^+(n,q)$ and $O^-(n,q)$ so that $O(Q) \cong O^+(n,q)$ if Q is of plus type and $O(Q) \cong O^-(n,q)$ if Q is of minus type.

Proof. By Lemma 2.22 we have that all non-singular quadratic forms are equivalent up to multiplication by a scalar when n is odd. It follows that there is one orthogonal group up to isomorphism in this case.

When n is even each non-singular quadratic form is equivalent to one of the two forms Q_+ and Q_- by Lemma 2.21. Denoting the Orthogonal group $O(Q_+)$ by $O^+(n,q)$ it follows that $O(Q)$ is isomorphic to $O^+(n,q)$ when Q is of plus type. Similarly denoting the group $O(Q_-)$ by $O^-(n,q)$ it follows that $O(Q)$ is isomorphic to $O^-(n,q)$ when Q is of minus type. Thus there are two Orthogonal groups up to isomorphism when n is even. □

Lemma 2.28. *When $n = 2s+1$ the order of the orthogonal group is*

$$|O(n,q)| = 2q^{s^2}\prod_{i=1}^{s}(q^{2i}-1).$$

When $n = 2s$ the orders of the orthogonal groups are

$$|O^{\pm}(n,q)| = 2q^{s(s-1)}(q^s \mp 1)\prod_{i=1}^{s-1}(q^{2i}-1).$$

These orders are given explicitly but without proof in Peter Cameron's lecture notes on Classical Groups which can be found on his webpage:

`www.maths.qmul.ac.uk/~pjc/class_gps/ch6.pdf`

The orders are also given in [12] Appendix I Table AI.1. and are explained as follows.

Table AI.1 gives the orders for groups $DX(n,q)$ for various D and X with respective invariants listed in canonical form on the ultimate line of the table.

For the Orthogonal groups $D = I$. When n is odd X is the group O with invariant $\mathcal{P}_{n-1}$ and when n is even X is the group O_+ with invariant $\mathcal{H}_{n-1}$ or O_- with invariant $\mathcal{E}_{n-1}$.

The canonical forms of the respective quadrics in $PG(n,q)$, the dimension n Projective space, $\mathcal{P}_{2s}, \mathcal{H}_{2s-1}, \mathcal{E}_{2s-1}$ are given in [12] in the statement of Theorem 5.16. The dimensions $2s$ of the Projective space corresponding to dimension $2s+1$ in Euclidean space and similarly that of $2s-1$ corresponding to $2s$. Thus we see that the group O corresponds to the one Orthogonal group $O(n,q)$ for n odd and the groups O_+ and O_- to the groups $O^+(n,q)$ and $O^-(n,q)$ respectively, for n even defined in the statement of Lemma 2.27.

- The order of the group O is then given in the Table AI.1 as $(q-1,2)$ with multiplier

$$F = q^{(n-1)/2} \times \lambda_1((n-1)/2, q^2).$$

The value of $(q-1,2)$, the greatest common divisor of $q-1$ and 2, is 2 as q is odd and the formula

$$\lambda_1(m,r) = r^{m(m-1)/2} \prod_{i=1}^{m} (r^i - 1)$$

is given in [12] §AI.3.

Thus

$$\begin{aligned}
|O(n,q)| &= 2q^{(n-1)/2} \times \lambda_1((n-1)/2, q^2) \\
&= 2q^s \times \lambda_1(s, q^2) \qquad \text{as } n = 2s+1 \\
&= 2q^s \times (q^2)^{s(s-1)/2} \prod_{i=1}^{s} ((q^2)^i - 1) \\
&= 2q^s q^{s(s-1)} \prod_{i=1}^{s} (q^{2i} - 1) \\
&= 2q^{s^2} \prod_{i=1}^{s} (q^{2i} - 1)
\end{aligned}$$

as required.

- Similarly the orders of the groups $O_\pm$ are given in the Table AI.1 as 2 with multipliers

$$F = q^{n-2}(q^{n/2} \mp 1) \times \lambda_1((n-2)/2, q^2).$$

Thus

$$\begin{aligned}
|O^\pm(n,q)| &= 2q^{n-2}(q^{n/2} \mp 1) \times \lambda_1((n-2)/2, q^2) \\
&= 2q^{2s-2}(q^s \mp 1) \times \lambda_1((s-1, q^2) \qquad \text{as } n = 2s \\
&= 2q^{2s-2}(q^s \mp 1) \times (q^2)^{(s-1)(s-2)/2} \prod_{i=1}^{s-1}((q^2)^i - 1) \\
&= 2q^{2s-2}q^{s^2-3s+2}(q^s \mp 1) \prod_{i=1}^{s-1}(q^{2i} - 1) \\
&= 2q^{s^2-s}(q^s \mp 1) \prod_{i=1}^{s-1}(q^{2i} - 1) \\
&= 2q^{s(s-1)}(q^s \mp 1) \prod_{i=1}^{s-1}(q^{2i} - 1)
\end{aligned}$$

as required.

Chapter 3

Invariants of the Orthogonal Group

We now consider the known invariants of the Orthogonal groups over finite fields of odd characteristic. In this chapter we consider known invariants in the general case being aware that there has been significant development of the theory of invariants of the Orthogonal group in some cases for small values of n. In particular we note the contributions of [7] and [8]. For the general case in §1 we review the Dickson invariants which being invariants of the General Linear group are thus invariants of the Orthogonal groups. In §2 we consider invariants generated from ξ_0, the quadratic form defining the orthogonal group, via the Steenrod operations. Then in §3 we introduce the Chern orbit classes of the Orthogonal group which are seen to be invariants. In later chapters we use these established invariants to generate new invariants.

3.1 The Dickson invariants

We introduce the Dickson Invariants as described by Clarence Wilkerson in [23].

The ring of invariants of the General Linear Group of an n dimensional vector space V over a finite field $\mathbb{F}_q$ where n is finite was computed by L E Dickson in [9] early in the 20th century and found to be a graded polynomial algebra generated by polynomials $c_{n,i}$, the *Dickson Invariants*.

The Dickson Invariants are generated by the *Dickson polynomial*

$$d_n(X) = \prod_{v \in V} (X - v)$$

with roots that are the elements of V.

It can be seen that $d_n(X)$ is invariant under the General Linear group $GL(V)$ as any element $g \in GL(V)$ merely permutes the vectors $v \in V$. It follows that the coefficients of powers of X in $d_n(X)$ are also invariant. These coefficients are the *Dickson Invariants*.

Lemma 3.1. *If the Dickson polynomial* $d_n(X) = \prod_{v \in V}(X - v)$ *then*

$$d_n(X) = X^{q^n} + \sum_{i=0}^{n-1}(-1)^{n-i}c_{n,i}X^{q^i}$$

for the Dickson invariants $c_{n,i} \in \mathbb{F}_q[V]$ *defined explicitly in the Equation 3.1.*

Proof. Denote by V_n the n dimensional vector space with basis $x_1, x_2, \ldots, x_n$ and define the *Dickson matrix*

$$D_n(X) = \begin{pmatrix} x_1 & x_2 & \ldots & x_n & X \\ x_1^q & x_2^q & \ldots & x_n^q & X^q \\ x_1^{q^2} & x_2^{q^2} & \ldots & x_n^{q^2} & X^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{q^n} & x_2^{q^n} & \ldots & x_n^{q^n} & X^{q^n} \end{pmatrix}$$

with

$$\Delta_n(X) = \det(D_n(X)).$$

Then each $v \in V_n$ is a root of the polynomial $\Delta_n(X)$ as can be seen by column operations on $D_n(X)$ as follows.

Let

$$v = \sum_{i=1}^{n} \alpha_i x_i$$

be an element of V_n.

Subtracting α_i multiples of column i from column $n+1$ in matrix $D_n(X)$ we have

$$\begin{aligned}\Delta_n(X) &= \begin{vmatrix} x_1 & \dots & x_n & X \\ x_1^q & \dots & x_n^q & X^q \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{q^n} & \dots & x_n^{q^n} & X^{q^n} \end{vmatrix} = \begin{vmatrix} x_1 & \dots & x_n & X - \sum \alpha_i x_i \\ x_1^q & \dots & x_n^q & X^q - \sum \alpha_i x_i^q \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{q^n} & \dots & x_n^{q^n} & X^{q^n} - \sum \alpha_i x_i^{q^n} \end{vmatrix} \\ &= \begin{vmatrix} x_1 & \dots & x_n & X - v \\ x_1^q & \dots & x_n^q & (X-v)^q \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{q^n} & \dots & x_n^{q^n} & (X-v)^{q^n} \end{vmatrix} \quad \text{by the Frobenius map.}\end{aligned}$$

Thus we see that each $v \in V$ is a root of the q^n degree polynomial $\Delta_n(X)$ and so we have identified all such roots.

The coefficient of X^{q^n} in $\Delta_n(X)$ is $\Delta_{n-1}(x_n)$ and so as $d_n(X)$ is monic we have

$$\Delta_n(X) = \Delta_{n-1}(x_n) d_n(X).$$

We aim to prove that the constant $\Delta_{n-1}(x_n)$ is non zero.

When $n = 1$ we have $\Delta_0(x_1) = x_1 \neq 0$ as the basis for the induction.

Now assume that $\Delta_{k-1}(x_k) \neq 0$ for all $k < n$.

Then

$$\begin{aligned}\Delta_{n-1}(X) &= \Delta_{n-2}(x_{n-1}) d_n(X) \\ &\neq 0 \quad \text{by the inductive hypothesis.}\end{aligned}$$

The roots of $\Delta_{n-1}(X)$ are the vectors of V_{n-1}, the $n-1$ dimensional space subspace of V with basis $x_1, x_2, \dots, x_{n-1}$. Thus x_n is not a root so $\Delta_{n-1}(x_n) \neq 0$.

Now denote by $\Gamma_{n,i}$ the determinant of the matrix $D_n(X)$ with the $i+1$th row and the $(n+1)$th column removed so that in particular $\Gamma_{n,n} = \Delta_{n-1}(x_n)$. Then

$$\Delta_n(X) = \sum_{i=0}^{n} (-1)^{n-i} \Gamma_{n,i} X^{q^i}.$$

Therefore

$$d_n(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i}$$

where each

$$(-1)^{n-i}c_{n,i} = \frac{(-1)^{n-i}\Gamma_{n,i}}{(-1)^{n-n}\Gamma_{n,n}} = (-1)^{n-i}\frac{\Gamma_{n,i}}{\Gamma_{n,n}}.$$

Thus

$$c_{n,i} = \frac{\Gamma_{n,i}}{\Gamma_{n,n}}. \tag{3.1}$$

□

Lemma 3.2. [21] *The ring $\mathbb{F}_q[c_0, c_1, c_2, c_3]$ is the ring of invariants of the General Linear Group $GL(4, 3)$.*

Lemma 3.3. *The degree of $c_{n,i}$ is $q^n - q^i$.*

Proof. The degree of $\Gamma_{n,i}$ is $-q^i + \sum_{j=0}^{n} q^j$ so that the degree of $\Gamma_{n,n}$ is $\sum_{j=0}^{n-1} q^j$.

Thus the degree of $c_{n,i}$ is $-q^i + \sum_{j=0}^{n} q^j - \sum_{i=0}^{n-1} q^j = q^n - q^i$ as required. □

Lemma 3.4. *Let $\ell = \Delta_{n-1}(x_n)$. Then the dickson invariant $c_{n,0} = \ell^{q-1}$.*

Proof. From the above proof we have that

$$\begin{aligned} c_{n,0} &= \frac{\Gamma_{n,0}}{\Gamma_{n,n}} \\ &= \frac{\begin{vmatrix} x_1^q & x_2^q & \dots & x_n^q \\ x_1^{q^2} & x_q^{q^2} & \dots & x_n^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{q^n} & x_2^{q^n} & \dots & x_n^{q^n} \end{vmatrix}}{\begin{vmatrix} x_1 & x_2 & \dots & x_n \\ x_1^q & x_2^q & \dots & x_n^q \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{q^n-1} & x_2^{q^{n-1}} & \dots & x_n^{q^n-1} \end{vmatrix}} \\ &= \frac{\ell^q}{\ell} = \ell^{q-1}. \end{aligned}$$

□

3.2 Invariants generated using the Steenrod Operations

Definition 3.5. Given a quadratic form

$$\xi_0 = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2$$

we define the associated homogeneous forms

$$\xi_j = \varepsilon x_1^{q^j+1} + \sum_{i=2}^{n} x_i^{q^j+1}.$$

We show that each of the forms ξ_j is an invariant of the Orthogonal group $O(\xi_0)$ by considering the action of the Steenrod operations on $S(V^*)$.

Definition 3.6. The *Steenrod operations*, $\mathcal{P}^n$ for each $n = 0, 1, 2, \ldots$, originally formulated as a refinement of the cup product in cohomology, act on $\mathbb{F}_q[V]$ forming the *Steenrod algebra* with the following properties:

(i) each $\mathcal{P}^k$ is a linear transformation,

(ii) $\mathcal{P}^0$ is the identity,

(iii) for each λ of degree 1 we have $\mathcal{P}^1\lambda = \lambda^q$ and $\mathcal{P}^k\lambda = 0$ if $k > 1$ and

(iv) the Cartan formula holds so that

$$\mathcal{P}^k\alpha\beta = \sum_{i=0}^{k} \mathcal{P}^i\alpha\mathcal{P}^{k-i}\beta.$$

As in [17] we view the Steenrod operations as a tool to use the information contained within the Frobenius homomorphism. (See Definition 2.11)

Lemma 3.7. *(i) $\mathcal{P}^k\alpha = 0$ if k is greater than the degree of α.*

(ii) Each $\mathcal{P}^k$ is homogeneous of degree $k(q-1)$.

Proof. We note that any form $\alpha \in \mathbb{F}_q[V]$ can be written as a linear combination of the products of linear forms. Thus we consider $\mathcal{P}^k(\lambda_1\lambda_2\ldots\lambda_j)$ for some $j > 0$ where each λ is a linear form in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

(i) We aim to prove, by induction on h, that

$$\mathcal{P}^{h+j}(\lambda_1\lambda_2\dots\lambda_h) = 0 \quad \text{if } j > 0 \tag{3.2}$$

for $h \in \mathbb{N}$.

We see that the statement is true when $h = 1$ by Definition 3.6 (iii).

Now assume the statement true for $h = \hat{h}$ that is

$$\mathcal{P}^{\hat{h}+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}}) = 0 \quad \text{if } j > 0. \tag{3.3}$$

For $h = \hat{h} + 1$ we have

$$\begin{aligned} P^{\hat{h}+1+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}+1}) &= \sum_{i=0}^{\hat{h}+1+j} \mathcal{P}^i(\lambda_1\lambda_2\dots\lambda_{\hat{h}})\mathcal{P}^{\hat{h}+1+j-i}(\lambda_{\hat{h}+1}) \\ &= \mathcal{P}^{\hat{h}+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}})\mathcal{P}^1(\lambda_{\hat{h}+1}) + \mathcal{P}^{\hat{h}+1+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}})\mathcal{P}^0(\lambda_{\hat{h}+1}) \end{aligned}$$

Now if $j > 0$

$$\mathcal{P}^{\hat{h}+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}}) = \mathcal{P}^{\hat{h}+1+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}}) = 0$$

by Equation 3.3.

Hence

$$P^{\hat{h}+1+j}(\lambda_1\lambda_2\dots\lambda_{\hat{h}+1}) = 0 \quad \text{if } j > 0.$$

Thus the statement is true for $h = \hat{h} + 1$ if true for $h = \hat{h}$ and so by induction the statement 3.2 is true for all $h \in \mathbb{N}$.

As each $\mathcal{P}^k$ is linear it follows that $\mathcal{P}^k\alpha = 0$ if k is greater than the degree of α.

(ii) Firstly we see that $\mathcal{P}^0$, the identity, is of degree 0 as required.

We aim to prove by induction on h that

$$\mathcal{P}^h(\lambda_1\lambda_2\dots\lambda_{h+j}) \text{ is homogeneous of degree } h + j + h(q-1) = hq + j \tag{3.4}$$

for $h \geq 1$, $j \geq 0$ and linear forms $\lambda_1, \dots, \lambda_{h+j}$.

We start by considering the case when $h = 1$ and aim to prove by induction on j that

$$\mathcal{P}^1(\lambda_1\lambda_2\dots\lambda_{1+j}) \text{ is homogeneous of degree } q + j \quad \text{for } j \geq 0. \tag{3.5}$$

When $j = 0$ we have that

$$\mathcal{P}^1(\lambda_1) = \lambda_1^q$$

which is of degree q as required.

Now assume that the statement 3.5 is true when $j = \hat{j}$ that is

$$\mathcal{P}^1(\lambda_1\lambda_2\ldots\lambda_{\hat{j}+1}) \text{ is homogeneous of degree } q+\hat{j} \quad \text{for } \hat{j} \geq 0. \tag{3.6}$$

When $j = \hat{j}+1$ with $\hat{j} \geq 0$ we have

$$\mathcal{P}^1(\lambda_1\lambda_2\ldots\lambda_{\hat{j}+2}) = \mathcal{P}^0(\lambda_1\lambda_2\ldots\lambda_{\hat{j}+1})\mathcal{P}^1(\lambda_{\hat{j}+2}) + \mathcal{P}^1(\lambda_1\lambda_2\ldots\lambda_{\hat{j}+1})\mathcal{P}^0(\lambda_{\hat{j}+2})$$

which by assumption 3.6 is homogeneous of degree $q+\hat{j}+1$ as required.

Thus statement 3.5 is proven.

How assume that statement 3.4 is true when $h = \hat{h}$. That is

$$\mathcal{P}^{\hat{h}}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}+j}) \text{ is homogeneous of degree } \hat{h}q+j \quad \text{for } j \geq 0. \tag{3.7}$$

We wish to deduce that

$$\mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}+j+1}) \text{ is homogeneous of degree } (\hat{h}+1)q+j \quad \text{for } j \geq 0. \tag{3.8}$$

We proceed by induction on j.

When $j = 0$ we have

$$\begin{aligned}\mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}+1}) &= \mathcal{P}^{\hat{h}}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}})\mathcal{P}^1(\lambda_{\hat{h}+1}) + \mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}})\mathcal{P}^0(\lambda_{\hat{h}+1}) \\ &= \mathcal{P}^{\hat{h}}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}})\mathcal{P}^1(\lambda_{\hat{h}+1}) + 0 \qquad \text{by Lemma 3.7.}\end{aligned}$$

We have that $\mathcal{P}^{\hat{h}}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}})$ is homogeneous of degree $\hat{h}q$ by equation 3.7.

Thus $\mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}+1})$ is homogeneous of degree $\hat{h}q+q = (\hat{h}+1)q$ as required.

Then assume that 3.8 is true when $j = \hat{j}$. That is

$$\mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2\ldots\lambda_{\hat{h}+\hat{j}+1}) \text{ is homogeneous of degree } (\hat{h}+1)q+\hat{j}. \tag{3.9}$$

Now

$$\mathcal{P}^{\hat{h}+1}(\lambda_1 \dots \lambda_{\hat{h}+\hat{j}+2}) \;=\; \mathcal{P}^{\hat{h}}(\lambda_1 \dots \lambda_{\hat{h}+\hat{j}+1})\mathcal{P}^1(\lambda_{\hat{h}+\hat{j}+2}) + \mathcal{P}^{\hat{h}+1}(\lambda_1 \dots \lambda_{\hat{h}+\hat{j}+1})\mathcal{P}^0(\lambda_{\hat{h}+\hat{j}+2}).$$

We have that $\mathcal{P}^{\hat{h}}(\lambda_1\lambda_2 \dots \lambda_{\hat{h}+\hat{j}+1})$ is homogeneous of degree $\hat{h}q + \hat{j} + 1$ by equation 3.7 and that $\mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2 \dots \lambda_{\hat{h}+\hat{j}+1})$ is homogeneous of degree $(\hat{h}+1)q + \hat{j}$ by equation 3.9. Thus $\mathcal{P}^{\hat{h}+1}(\lambda_1\lambda_2 \dots \lambda_{\hat{h}+\hat{j}+2})$ is homogeneous of degree $(\hat{h}+1)q + \hat{j} + 1$ as required.

Thus we have proven statement 3.4 as required.

As $\mathcal{P}^k$ is linear it follows for any $\alpha \in \mathbb{F}_q[V]$ that $\mathcal{P}^k(\alpha)$ is homogeneous of degree $k(q-1)+\deg(\alpha)$ so that $\mathcal{P}^k$ is of degree $k(q-1)$ as required.

□

We introduce the following map as defined in Section 8.1 of [17] in order to deduce further properties of the operators $\mathcal{P}^i$.

Definition 3.8. Define the map

$$\mathcal{P}(\zeta) : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V][[\zeta]]$$

such that

$$\mathcal{P}(\zeta) = \sum_{i=0}^{\infty} \mathcal{P}^i \zeta^i$$

where the $\mathcal{P}^i$ are the Steenrod operators as in Definition 3.6.

Lemma 3.9. *The map $\mathcal{P}(\zeta)$ is a ring homomorphism.*

Proof. For each $\alpha, \beta \in \mathbb{F}_q(V)$ we have the following.

(i) As each $\mathcal{P}^k$ is linear

$$\begin{aligned}
\mathcal{P}(\zeta)(\alpha+\beta) &= \sum_{k=0}^{\infty} \mathcal{P}^k(\alpha+\beta)\zeta^k \\
&= \sum_{k=0}^{\infty} (\mathcal{P}^k(\alpha) + \mathcal{P}^k(\beta))\zeta^k \\
&= \sum_{k=0}^{\infty} \mathcal{P}^k(\alpha)\zeta^k + \mathcal{P}^k(\beta)\zeta^k \\
&= \mathcal{P}(\zeta)(\alpha) + \mathcal{P}(\zeta)(\beta)).
\end{aligned}$$

(ii) From Definition 3.6 we have the Cartan formula

$$\mathcal{P}^k(\alpha\beta) = \sum_{i=0}^{k} \mathcal{P}^i(\alpha)\mathcal{P}^{k-i}(\beta).$$

Thus

$$\mathcal{P}(\zeta)(\alpha\beta) = \sum_{k=0}^{\infty}\sum_{i=0}^{k} \mathcal{P}^i(\alpha)\mathcal{P}^{k-i}(\beta)\zeta^k.$$

Setting the convention that

$$\mathcal{P}^i = 0 \quad \text{if } i < 0$$

we have

$$\begin{aligned} \mathcal{P}(\zeta)(\alpha\beta) &= \sum_{i,k\in\mathbf{Z}} \mathcal{P}^i(\alpha)\mathcal{P}^{k-i}(\beta)\zeta^k \\ &= \sum_{i,k\in\mathbf{Z}} \mathcal{P}^i(\alpha)\zeta^i \ \ \mathcal{P}^{k-i}(\beta)\zeta^{k-i} \\ &= \mathcal{P}(\zeta)(\alpha)\cdot\mathcal{P}(\zeta)(\beta). \end{aligned}$$

(iii) $\mathcal{P}(\zeta)(1) = 1$.

Thus $\mathcal{P}(\zeta)$ is a ring homomorphism. □

Lemma 3.10. *The ring homomorphism $\mathcal{P}(\zeta)$ is such that each linear form $x \in S(V^*)$ maps to $x + x^q\zeta$.*

Proof. Following Definition 3.6 we have, for each x of degree 1,

$$\mathcal{P}^i(x) = \begin{cases} x & \text{for } i = 0 \\ x^q & \text{for } i = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Thus, by definition

$$\mathcal{P}(\zeta)(x) = x + x^q\zeta$$

as required. □

Definition 3.11. We now define the Total Steenrod Operation $\mathcal{P}^\bullet$ as the alternating sum of the Steenrod operations. That is

$$\begin{aligned} \mathcal{P}^\bullet &= \mathcal{P}(-1) \\ &= \mathcal{P}^0 - \mathcal{P}^1 + \mathcal{P}^2 - \dots. \end{aligned}$$

We see that $\mathcal{P}^\bullet$ is a ring homomorphism.

Corollary 3.12. *The Total Steenrod Operation acts on the ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ such that*

$$\mathcal{P}^\bullet(x_i) = x_i - x_i^q \qquad i = 1, 2 \ldots, n.$$

Lemma 3.13. *The Total Steenrod Operation acts on the ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ such that*

(i) $\mathcal{P}^\bullet(\xi_0) = \xi_0 - 2\xi_1 + \xi_0^q$,

(ii) $\mathcal{P}^\bullet(\xi_k) = \xi_k - \xi_{k-1}^q - \xi_{k+1} + \xi_k^q$, *for all* $k \geq 1$

where the ξ_k are given in Definition 3.5.

Proof. We prove this in the case when

$$\xi_0 = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2 \quad \text{so that} \quad \xi_i = \varepsilon x_1^{q^i+1} + \sum_{i=2}^{n} x_i^{q^i+1}.$$

(i)

$$\begin{aligned}
\mathcal{P}^\bullet(\xi_0) &= \mathcal{P}^\bullet(\varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2) \\
&= \varepsilon(\mathcal{P}^\bullet(x_1))^2 + \sum_{i=2}^{n}(\mathcal{P}^\bullet(x_i))^2 \quad \text{as } \mathcal{P}^\bullet \text{ is a ring homomorpism} \\
&= \varepsilon(x_1 - x_1^q)^2 + \sum_{i=2}^{n}(x_i - x_i^q)^2 \quad \text{by Corollary 3.12} \\
&= \varepsilon(x_1^2 - 2x_1^{q+1} + x_1^{2q}) + \sum_{i=2}^{n} x_i^2 - 2x_i^{q+1} + x_i^{2q} \\
&= \left(\varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2\right) - 2\left(\varepsilon x_1^{q+1} + \sum_{i=2}^{n} x_i^{q+1}\right) + \left(\varepsilon x_1^{2q} + \sum_{i=2}^{n} x_i^{2q}\right) \\
&= \left(\varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2\right) - 2\left(\varepsilon x_1^{q+1} + \sum_{i=2}^{n} x_i^{q+1}\right) + \left(\varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2\right)^q \quad \text{since } \varepsilon = \varepsilon^q \\
&= \xi_0 - 2\xi_1 + \xi_0^q \quad \text{as required.}
\end{aligned}$$

(ii)

$$\begin{aligned}
\mathcal{P}^\bullet(\xi_k) &= \mathcal{P}^\bullet(\varepsilon x_1^{q^k+1} + \sum_{i=2}^n x_i^{q^k+1}) \\
&= \varepsilon(\mathcal{P}^\bullet(x_1))^{q^k+1} + \sum_{i=2}^n (\mathcal{P}^\bullet(x_i))^{q^k+1} \quad \text{as } \mathcal{P}^\bullet \text{ is a ring homomorpism} \\
&= \varepsilon(x_1 - x_1^q)^{q^k+1} + \sum_{i=2}^n (x_i - x_i^q)^{q^k+1} \\
&= \varepsilon(x_1 - x_1^q)(x_1 - x_1^q)^{q^k} + \sum_{i=2}^n (x_i - x_i^q)(x_i - x_i^q)^{q^k} \\
&= \varepsilon(x_1 - x_1^q)(x_1^{q^k} - x_1^{q^{k+1}}) + \sum_{i=2}^n (x_i - x_i^q)(x_i^{q^k} - x_i^{q^{k+1}}) \\
&= \varepsilon(x_1^{q^k+1} - x_1^{q^k+q} - x_1^{q^{k+1}+1} + x_1^{q^{k+1}+q}) \\
&\qquad + \sum_{i=2}^n (x_i^{q^k+1} - x_i^{q^k+q} - x_i^{q^{k+1}+1} + x_i^{q^{k+1}+q}).
\end{aligned}$$

Then since $\varepsilon = \varepsilon^q$

$$\begin{aligned}
\mathcal{P}^\bullet(\xi_0) &= \left(\varepsilon x_1^{q^k+1} + \sum_{i=2}^n x_i^{q^k+1}\right) - \left(\varepsilon x_1^{q^{k-1}+1} + \sum_{i=2}^n x_i^{q^{k-1}+1}\right)^q \\
&\qquad - \left(\varepsilon x_1^{q^{k+1}+1} + \sum_{i=2}^n x_i^{q^{k+1}+1}\right) + \left(\varepsilon x_1^{q^k+1} + \sum_{i=2}^n x_i^{q^k+1}\right)^q \\
&= \xi_k - \xi_{k-1}^q - \xi_{k+1} + \xi_k^q \quad \text{as required.}
\end{aligned}$$

□

Lemma 3.14. *The Steenrod algebra acts on the ring* $\mathbb{F}_q[\xi_0, \xi_1, \xi_2, \dots]$ *such that*

(i) $\mathcal{P}^0(\xi_k) = \xi_k$ *for each* $k = 0, 1, 2, \dots,$

(ii) $\mathcal{P}^1(\xi_0) = 2\xi_1$ *and* $\mathcal{P}^1(\xi_k) = \xi_{k-1}^q$ *for each* $k = 1, 2, \dots,$

(iii) $\mathcal{P}^{q^k}(\xi_k) = \xi_{k+1}$ *for each* $k = 1, 2, \dots$

(iv) $\mathcal{P}^{q^k+1}(\xi_k) = \xi_k^q$ *for each* $k = 0, 1, \dots$ *and*

(v) $\mathcal{P}^i(\xi_k) = 0$ *otherwise.*

Proof. We have that $\mathcal{P}^k$ is homogeneous of degree $k(q-1)$ by Lemma 3.7 (ii) and so consider the degrees of the terms in $\mathcal{P}^\bullet(\xi_k)$.

Since $\mathcal{P}^k(\xi_0) = 0$ for all $k \geq 3$ by Lemma 3.7 (i), we have by Lemma 3.13 (i):

$$\mathcal{P}^\bullet(\xi_0) = \mathcal{P}^0(\xi_0) - \mathcal{P}^1(\xi_0) + \mathcal{P}^2(\xi_0) = \xi_0 - 2\xi_1 + \xi_0^q.$$

The degrees of ξ_0, ξ_0^q and ξ_1 are 2, $2q$ and $q+1$ respectively and by Lemma 3.7 $\mathcal{P}^k(\xi_0)$ is homogeneous of degree $2 + k(q-1)$.

Then

- $\deg(\mathcal{P}^0(\xi_0)) = 2$ so $\mathcal{P}^0(\xi_0) = \xi_0$ as expected as $\mathcal{P}^0$ is the identity.
- $\deg(\mathcal{P}^1(\xi_0)) = 2 + q - 1 = q + 1$ so $\mathcal{P}^1(\xi_0)) = 2\xi_1$
- $\deg(\mathcal{P}^{q^0+1}(\xi_0)) = 2 + 2(q-1) = 2q$ so $\mathcal{P}^2(\xi_0)) = \xi_0^q$
- $\deg(\mathcal{P}^i(\xi_0)) = 0$ otherwise.

Now

$$\mathcal{P}^\bullet(\xi_k) = \mathcal{P}^0(\xi_k) - \mathcal{P}^1(\xi_k) + \mathcal{P}^2(\xi_k) - \cdots = \xi_k - \xi_{k-1}^q - \xi_{k+1} + \xi_k^q$$

by Lemma 3.13 (ii).

The degrees of ξ_k, ξ_{k-1}^q, ξ_{k+1} and ξ_k^q are $q^k + 1$, $q^k + q$, $q^{k+1} + 1$ and $q^{k+1} + q$ respectively and by Lemma 3.7 $\mathcal{P}^k(\xi_j)$ is homogeneous of degree $q^j + 1 + k(q-1)$.

Then

- $\deg(\mathcal{P}^0(\xi_k)) = q^k + 1$ so $\mathcal{P}^0(\xi_k) = \xi_k$ as expected as $\mathcal{P}^0$ is the identity, thus completing the proof of (i);
- $\deg(\mathcal{P}^1(\xi_k)) = q^k + 1 + (q-1) = q^k + q$ so $\mathcal{P}^1(\xi_k)) = \xi_{k-1}^q$, completing the proof of (ii);
- $\deg(\mathcal{P}^{q^k}(\xi_k)) = q^k + 1 + q^k(q-1) = q^{k+1} + 1$ so $\mathcal{P}^{q^k}(\xi_k)) = \xi_{k+1}$, proving (iii);
- $\deg(\mathcal{P}^{q^k+1}(\xi_k)) = q^k + 1 + (q^k+1)(q-1) = q^{k+1} + q$ so $\mathcal{P}^{q^k+1}(\xi_k)) = \xi_k^q$, proving (iv) and
- $\mathcal{P}^i(\xi_k) = 0$ otherwise, proving (v).

□

Lemma 3.15 ([17] Section 8.1)**.** *The Steenrod Operations $\mathcal{P}^i$ map invariant forms to invariant forms.*

Corollary 3.16. *Each ξ_j defined from ξ_0 as in Definition 3.2 is an invariant of the Orthogonal group $O(\xi_0)$.*

Proof. This follows with reference to Lemma 3.14 (ii) and (iii). □

3.3 Chern Orbit Classes

The Chern Orbit Classes for a given group are presented in [18] Section 1 as a tool for generating invariants of the group.

Let V be an n dimensional vector space over $\mathbb{F}_q$ and $G \leq GL(V)$ so that G is a finite group. We consider the action of G on V^*, the dual of V, and in particular the G orbits of V^*.

Definition 3.17. Let $\mathcal{O}^* \subseteq V^*$ be a G orbit and set

$$\chi_{\mathcal{O}^*}(X) = \prod_{x \in \mathcal{O}^*} (X + x)$$

The polynomial $\chi_{\mathcal{O}^*}(X)$ is the *Orbit polynomial* of the orbit $\mathcal{O}^*$.

If $|\mathcal{O}^*|$ denotes the cardinality of $\mathcal{O}^*$ then

$$\chi_{\mathcal{O}^*}(X) = \sum_{i+j=|\mathcal{O}^*|} c_i(\mathcal{O}^*) X^j$$

and the coefficients $c_i(\mathcal{O}^*),\ i = 1, \ldots |\mathcal{O}^*|$ are the *Chern Orbit Classes* of the orbit $\mathcal{O}^*$.

Lemma 3.18 ([18] Lemma 1.1)**.** *If $\mathcal{O}^* \subseteq V$ is an orbit of G then the coefficients $c_i(\mathcal{O}^*)$ of $\chi_{\mathcal{O}^*}(X)$ which are homogeneous polynomials in $S(V^*)$ of degree i for $i = 1, 2, \ldots, |\mathcal{O}^*|$ are invariant under the action of G on the Symmetric Algebra on the dual of V.*

Being concerned with the invariants of the Orthogonal group we let $G = O(\xi_0)$.

We require a method for calculating the coefficients $c_i(\mathcal{O}^*)$ for each of the $O(\xi_0)$ orbits of V^* without explicitly calculating the Orthogonal group. To this end we evaluate the form ξ_0 on the vectors of V identifying the set of vectors on which the form is equal to a given element of $\mathbb{F}_q$. For each element of $\mathbb{F}_q$ we show that the corresponding set of vectors $\hat{Q}(v) \in V^*$ is an $O(\xi_0)$ orbit of V^*, where $\hat{Q}$ is the map from V to V^* determined by the quadratic form defined in Section 1.3.

Lemma 3.19. *Let $\hat{Q}$ be the map from V to V^* determined by the quadratic form ξ_0 as defined in Lemma 1.23. Then we have*

$$\hat{Q}(gv) = \hat{Q}(v)^{g^{-1}}.$$

Proof. Let b be the polarisation of the quadratic form ξ_0. Then $\xi_0(v) = b(v, v)$ and so $\hat{Q}(v) = b(v, \cdot)$.

Thus for $g \in O(\xi_0)$

$$\begin{aligned}
\hat{Q}(gv)(u) &= b(gv, u) \\
&= b(v, g^{-1}u) \quad \text{as } g \in O(\xi_0) \\
&= \hat{Q}(v)(g^{-1}(u)) \\
&= \hat{Q}(v)g^{-1}(u) \\
&= \hat{Q}(v)^{g^{-1}}(u)
\end{aligned}$$

Thus $\hat{Q}(gv) = \hat{Q}(v)^{g^{-1}}$. □

Lemma 3.20. *Given a quadratic form ξ_0 and some $j \in \mathbb{F}_q$ let $\mathcal{O}_j = \{v \in V | \xi_0(v) = j\}$ and $\mathcal{O}_j^* = \{\hat{Q}(v) \in V^* | v \in \mathcal{O}_j\}$. Then $\mathcal{O}_j^*$ is the union of orbits $O(\xi_0)$ of V^*.*

Proof. Choose $v \in V$ such that $\xi_0(v) = j$ and let $x \in V^*$ be such that $\hat{Q}(v) = x$. Define $\mathcal{O}_x$ as the orbit $O(\xi_0)$ of V^* containing x so that $\mathcal{O}_x = \{x^g | g \in O(\xi_0)\}$.

Then for each $x^g \in \mathcal{O}_x$ we have

$$\begin{aligned}
\xi_0(\hat{Q}^{-1}(x^g)) &= \xi_0(hv) \quad \text{where } h = g^{-1} \in O(\xi_0) \\
&= \xi_0^h(v) = \xi_0(v) \quad ash \in O(\xi_0) \\
&= j.
\end{aligned}$$

Thus we have $x^g \in \mathcal{O}_j^*$ so $\mathcal{O}_x \subset \mathcal{O}_j^*$.

If now there exists some $y \in \mathcal{O}_j^*$ such that $y \notin \mathcal{O}_x$ and $y = \hat{Q}(u)$ for some $u \in V$ where $\xi_0(u) = j$, then for each $y^g \in \mathcal{O}_x$ we have

$$\xi_0(\hat{Q}^{-1}(y^g)) = \xi_0(g^{-1}u) = \xi_0^g(u) = \xi_0(u) = j.$$

Thus $y^g \in \mathcal{O}_j^*$ so $\mathcal{O}_x \cup \mathcal{O}_y \subset \mathcal{O}_j^*$.

We continue thus until all elements of the orbit $\mathcal{O}_j^*$ are accounted for and thus see that $\mathcal{O}_j^*$ is the union of orbits $O(\xi_0)$ of V^* as required. □

Thus the polynomial

$$\chi_{\mathcal{O}_j^*}(X) = \prod_{x \in \mathcal{O}_j^*} (X + x)$$

being a product of chern orbit polynomials has coefficients that are invariants of the Orthogonal group.

Lemma 3.21. *The subsets $\mathcal{O}_j^*$ of V^* for $j \neq 0$ are $O(\xi_0)$ orbits of V^*.*

Proof. This follows from Lemma 3.19. □

Being concerned to discover any relationships between the established invariants of the orthogonal group we used CoCoA code to discover which of the Chern Orbit Classes can be written as a polynomial in the ξ_k polynomials of Definition 3.5 and on discovering that some could not in the cases $n = 3$ and $n = 4$ we propose the following conjecture.

Conjecture 3.22. Given ξ_0 and related polynomials ξ_k of Definition 3.5 then for some j there are Chern orbit classes of $\mathcal{O}_j^*$ that cannot be written as polynomials in the ξ's.

In particular such Chern orbit classes exist of degree $\frac{q^n - q^{n-i}}{q}$ for some values of $1 \leq i < n$.

We have shown this conjecture to be true when $n = 3$ and $n = 4$ for small values of q using CoCoA code. The code and results are given in Appendix A. An example of the code for $n = 3$ is given in Appendix A.1 with output from this code for the cases $q = 3, 5, 7, 11$ when the quadratic form is $x_1^2 + x_2^2 + x_3^2$ given in Appendix A.2. Output from similar code for the case $n = 4$ and $q = 3$ is given in Appendix A.3.

We see that when $n = 4$, $q = 3$ and $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ we have Chern orbit classes of degree $\frac{q^n - q^{n-1}}{q} = 18$ and of degree $\frac{q^n - q^{n-2}}{q} = 24$ that cannot be written as a polynomials in the ξ's. Thus we make the following definitions for use in later chapters.

Definition 3.23. Let $n = 4$, $q = 3$ and $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Then define h_i to be the Chern Orbit Class of degree $\frac{q^n - q^{n-i}}{q}$ of the polynomial $\chi_{\mathcal{O}_0^*}(X)$ defined above for $i = 2, 3$ so that h_3 is of degree 18 and h_2 of degree 24.

The polynomials h_2 and h_3 are given explicitly in Appendix A.4.

Chapter 4

Generation of some new invariants

In the previous chapter in §3.3 we saw that there exists Chern orbit classes of degrees $\frac{q^n-q^{n-i}}{q}$ for some $1 \leq i < n$ that can not be expressed in terms of the polynomials ξ_k, as given in Definition 3.5, in some cases for small values of n and q. In this chapter we take this as motivation to investigate the existence of additional invariants of the Orthogonal group of these degrees. We note with reference to Lemma 3.3 that of the Dickson invariants $c_{n,i}$ the invariant $c_{n,n-1}$ has degree $q^n - q^{n-1}$. Thus we investigate for given n whether the polynomial $c_{n,n-1}$ can be adjusted by adding a polynomial in the ξ_k's in order that the resulting polynomial is a qth power. We extend this idea to the other Dickson invariants. In §1 we present a conjecture asserting that such an polynomial exists maintaining that the qth root of the polynomial is an invariant of the Orthogonal group. Then in §2 we present the proof of the conjecture when $n = 2$ and in later sections we investigate the truth of the conjecture for $n = 3$ and $n = 4$ for small values of q.

4.1 The d_i invariants

Given a vector space of dimension n over a finite field of q elements with q odd we choose a non singular quadratic form ξ_0 and thus determine the Orthogonal group $O(\xi_0)$.

We aim to establish a new invariant of $O(\xi_0)$ by utilization of the Frobenius automorphism and the known invariants of the Orthogonal group; the Dickson Invariants $c_{n,i}$ presented in §3.1 and the forms ξ_k, derived from ξ_0 using the Steenrod Algebra, presented in §3.2. Having fixed the dimension n of the vector space V we adopt the notation c_i for the ith Dickson invariant.

Given a quadratic form ξ_0, if there exists a polynomial ϕ_i in the forms ξ_j such that the sum of c_i and ϕ_i is a qth power then $c_i + \phi_i$ is an invariant of $O(\xi_0)$. It follows by application of the Frobenius automorphism that the qth root of this polynomial must also be an invariant. Thus we present the following conjecture.

Conjecture 4.1. Let $O(\xi_0)$ be the orthogonal group determined by the non-singular quadratic form ξ_0 in n variables over the finite field $\mathbb{F}_q$. Then for each c_i there exists a polynomial ϕ_i in the forms $\xi_0, \xi_1, \ldots, \xi_{n-1}$ such that

$$c_i + \phi_i = d_i^q$$

for some polynomial d_i.

Then d_i is an invariant of $O(\xi_0)$.

We note that we need consider ϕ_i only as a polynomial in the forms ξ_k for $k = 0, 1, \ldots n-1$ as ξ_n has degree $q^n + 1$ which is greater than $q^n - q^i$, the degree of the $c_{n,i}$, for all values of i.

We investigate the truth of this conjecture for $i = n - 1$. This value of i gives the lowest degree polynomial of the c_i's. The d_i's for $i = 0, 1, \ldots, n-2$ can be obtained from c_{n-1} by application of the Steenrod operations.

4.2 Proof of Conjecture 4.1 in the case $n = 2$

Maple code was used to investigate the truth of Conjecture 4.1 in the case $n = 2$ and $i = 1$ and the results generalised. Thus we are able to present the following theorem.

Theorem 4.2. *Let V be a vector space of dimension 2 over $\mathbb{F}_q$ with q odd and let x, y be a basis for V. Define c_1 to be the 1st Dickson Invariant and let the quadratic form $\xi_0 = x^2 + \varepsilon y^2$. Then the polynomial*

$$\phi_1 = \frac{-1}{\varepsilon^{\frac{q-1}{2}}} \frac{\xi_1}{\xi_0^q} (\xi_0^{q+1} - \xi_1^2)^{\frac{q-1}{2}} + \left[\frac{-1}{\varepsilon}\right]^{\frac{q-1}{2}} \frac{\xi_1^q}{\xi_0^q}$$

is such that the polynomial $c_1 + \phi_1$ is the qth power d_1^q.

The qth root of $c_1 + \phi_1$, the polynomial d_1 in the basis vectors of V is an invariant of $O(\xi_0)$.

If ξ_0 is of minus type then

$$d_1 = 0$$

and if ξ_0 is of plus type then

$$d_1 = 2\frac{\xi_1}{\xi_0} = 2(x^{q-1} - \varepsilon x^{q-3}y^2 + \cdots + (-\varepsilon)^{\frac{q-3}{2}} x^2 y^{q-3} + (-\varepsilon)^{\frac{q-1}{2}} y^{q-1}).$$

Proof. Given $\xi_0 = x_1^2 + \varepsilon y_1^2$ then $\xi_1 = x_1^{q+1} + \varepsilon y_1^{q+1}$.

Hence

$$\begin{aligned}
(\xi_0^{q+1} - \xi_1^2)^{\frac{q-1}{2}} &= (\xi_0^q \xi_0 - \xi_1^2)^{\frac{q-1}{2}} = \left[(x^{2q} + \varepsilon y^{2q})(x^2 + \varepsilon y^2) - (x^{q+1} + \varepsilon y^{q+1})^2\right]^{\frac{q-1}{2}} \\
&= \left[x^{2q+2} + \varepsilon x^{2q} y^2 + \varepsilon x^2 y^{2q} + \varepsilon^2 y^{2q+2} - (x^{2q+2} + 2\varepsilon x^{q+1} y^{q+1} + \varepsilon^2 y^{2q+2})\right]^{\frac{q-1}{2}} \\
&= \left(\varepsilon x^{2q} y^2 + \varepsilon x^2 y^{2q} - 2\varepsilon x^{q+1} y^{q+1}\right)^{\frac{q-1}{2}} \\
&= \varepsilon^{\frac{q-1}{2}} x^{q-1} y^{q-1} \left(x^{2q-2} + y^{2q-2} - 2x^{q-1} y^{q-1}\right)^{\frac{q-1}{2}} \\
&= \varepsilon^{\frac{q-1}{2}} x^{q-1} y^{q-1} \left(x^{q-1} - y^{q-1}\right)^{q-1} = \varepsilon^{\frac{q-1}{2}} x^{q-1} y^{q-1} \frac{\left(x^{q-1} - y^{q-1}\right)^q}{x^{q-1} - y^{q-1}}.
\end{aligned}$$

It follows that

$$\begin{aligned}
c_1 + \frac{-1}{\varepsilon^{\frac{q-1}{2}}} \frac{\xi_1}{\xi_0^q} (\xi_0^{q+1} - \xi_1^2)^{\frac{q-1}{2}} &= \frac{x^{q^2-1} - y^{q^2-1}}{x^{q-1} - y^{q-1}} - \frac{1}{\varepsilon^{\frac{q-1}{2}}} \frac{\xi_1}{\xi_0^q} \varepsilon^{\frac{q-1}{2}} x^{q-1} y^{q-1} \frac{\left(x^{q-1} - y^{q-1}\right)^q}{x^{q-1} - y^{q-1}} \\
&= \frac{x^{q^2-1} - y^{q^2-1}}{x^{q-1} - y^{q-1}} - \frac{x^{q+1} + \varepsilon y^{q+1}}{(x^2 + \varepsilon y^2)^q} x^{q-1} y^{q-1} \frac{\left(x^{q-1} - y^{q-1}\right)^q}{x^{q-1} - y^{q-1}}
\end{aligned}$$

$$\begin{aligned}
&= \frac{(x^{q^2-1} - y^{q^2-1})(x^{2q} + \varepsilon y^{2q}) - (x^{q+1} + \varepsilon y^{q+1}) x^{q-1} y^{q-1} (x^{q(q-1)} - y^{q(q-1)})}{(x^{q-1} - y^{q-1})(x^{2q} + \varepsilon y^{2q})} \\
&= \frac{x^{q^2+2q-1} - x^{q^2+q} y^{q-1} - \varepsilon y^{q^2+2q-1} + \varepsilon x^{q-1} y^{q^2+q}}{(x^{q-1} - y^{q-1})(x^{2q} + \varepsilon y^{2q})} \\
&= \frac{(x^{q^2+q} + \varepsilon y^{q^2+q})(x^{q-1} - y^{q-1})}{(x^{q-1} - y^{q-1})(x^{2q} + \varepsilon y^{2q})} = \frac{(x^{q+1} + \varepsilon y^{q+1})^q}{(x^2 + \varepsilon y^2)^q} = \frac{\xi_1^q}{\xi_0^q}.
\end{aligned}$$

So we have

$$c_1 + \phi_1 = \frac{\xi_1^q}{\xi_0^q} + \left[\frac{-1}{\varepsilon}\right]^{\frac{q-1}{2}} \frac{\xi_1^q}{\xi_0^q} = \left[1 + \left(\frac{-1}{\varepsilon}\right)^{\frac{q-1}{2}}\right] \frac{\xi_1^q}{\xi_0^q}.$$

Let ξ_0 be of minus type.

(i) If $q \equiv 3 \bmod 4$, ε must be a square in $\mathbb{F}_q$ and since -1 is a non square we have $\varepsilon^{\frac{q-1}{2}} = 1$ and $(-1)^{\frac{q-1}{2}} = -1$.

(ii) If $q \equiv 1 \bmod 4$, ε must be a non square in $\mathbb{F}_q$ and since -1 is a square we have $(-1)^{\frac{q-1}{2}} = 1$ and $\varepsilon^{\frac{q-1}{2}} = -1$.

Hence, in either case, $\left(\frac{-1}{\varepsilon}\right)^{\frac{q-1}{2}} = -1$ so $c_1 + \phi_1 = d_1^q = 0$ and $d_1 = 0$ as required.

Let ξ_0 be of plus type.

(i) If $q \equiv 3 \bmod 4$ then ε must be a non square in $\mathbb{F}_q$ so that $\varepsilon^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} = -1$.

(ii) If $q \equiv 1 \bmod 4$ then ε must be a square in $\mathbb{F}_q$ so that $\varepsilon^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} = 1$.

Hence, in either case, $\left(\frac{-1}{\varepsilon}\right)^{\frac{q-1}{2}} = 1$ so that $c_1 + \phi_1 = d_1^q = 2\frac{\xi_1^q}{\xi_0^q}$.

It follows that

$$d_1 = 2\frac{\xi_1}{\xi_0} = 2(x^{q-1} - \varepsilon x^{q-3}y^2 + \cdots + (-\varepsilon)^{\frac{q-3}{2}}x^2y^{q-3} + (-\varepsilon)^{\frac{q-1}{2}}y^{q-1})$$

as required.

□

We note that the results of Theorem 4.2 are consistent with those of [8]: Theorem B.

4.3 An algorithm to test Conjecture 4.1

We present an algorithm to determine the polynomial ϕ_i and the associated form d_i of Conjecture 4.1 for $n = 4$, $q = 3$ and form $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

- Preliminaries: the degree of c_i is calculated and the ξ_k's are determined for $k = 1 \ldots n-1$. The degree of ξ_k is greater than that of c_i for $k \geq n$.

- The expressions

  $$g(\alpha, \beta, \gamma) = \xi_3^\alpha \xi_2^\beta \xi_1^\gamma \xi_0^\delta$$

  are determined such that the total degree of the expression is equal to that of the Dickson invariant c_i. As such an expression is itself a qth power when each of the degrees α, β, γ and δ are multiples of q these expressions are not used in the calulation.

  A matrix D is created to hold the values of $\alpha, \beta, \gamma, \delta$ for all possible expressions that are not qth powers.

- The coefficients of the terms $x_1^a x_2^b x_3^c x_4^d$ are extracted from each $g(\alpha, \beta, \gamma)$ to form a row vector. As the form ξ_0 is a symmetric polynomial in the ξ_i's the polynomials $g(\alpha, \beta, \gamma)$ are also symmetric. Thus we only need consider terms $x_1^a x_2^b x_3^c x_4^d$ with $a \geq b \geq c \geq d$.

  Again, as a $x_1^a x_2^b x_3^c x_4^d$ term is itself a qth power when each of the degrees a, b, c and d are multiples of q the coefficients of these terms are not used in the calculation.

- The polynomial c_i is determined from the Dickson matrix as presented in the proof of Lemma 3.1 and the coefficients extracted to form a row vector as above.

- A matrix is formed from the row vectors and the transpose of this matrix is reduced to Row-Reduced Echelon Form. If the system of equations leads to a single solution the redundant zero rows of the matrix are removed and a solution vector, s, defined as the transpose of the final column of the resulting matrix. This solution vector s then gives gives the coefficients of the relevant terms $g(\alpha, \beta, \gamma)$ in the polynomial ϕ_i.

- The matrix D and vector s are then used to give the polynomial ϕ_i explicitly as a polynomial in the ξ_k's.

- The form d_i^q is then calculated explicitly as a polynomial in the variables x_i and the qth root calculated to give the desired d_i.

4.4 The ϕ_2 and d_2 polynomials for $n = 3$

Using code for an algorithm similar to that given in §4.3 but for $n = 3$ and $i = 2$ we have shown Conjecture 4.1 to be true for $q = 3, 5, 7, 9$ with $\xi_0 = x_1^2 + x_2^2 + x_3^2$ in each case and have the following polynomials ϕ_2.

- $q = 3$

$$\phi_2 = \xi_2\xi_1^2 + 2\xi_2\xi_0^4 + \xi_1^4\xi_0$$

- $q = 5$

$$\begin{aligned}\phi_2 &= \xi_2^3\left[3\xi_1^2\xi_0^5 + 2\xi_0^{11}\right] + \xi_2^2\left[\xi_1^8 + 4\xi_1^6\xi_0^6\right] \\ &+ \xi_2\left[4\xi_1^{12}\xi_0 + \xi_1^{10}\xi_0^7 + 4\xi_1^4\xi_0^{25} + 2\xi_1^2\xi_0^{31} + 4\xi_0^{37}\right] \\ &+ \left[4\xi_1^{16}\xi_0^2 + 3\xi_1^8\xi_0^{26} + \xi_1^6\xi_0^{32}\right]\end{aligned}$$

- $q = 7$

$$\begin{aligned}\phi_2 &= \xi_2^5\left[4\xi_1^2\xi_0^{14} + 3\xi_0^{22}\right] + \xi_2^4\left[\xi_1^{10}\xi_0^7 + 6\xi_1^8\xi_0^{15}\right] \\ &+ \xi_2^3\left[\xi_1^{18} + 3\xi_1^{16}\xi_0^8 + 3\xi_1^{14}\xi_0^{16} + 4\xi_1^4\xi_0^{56} + 6\xi_1^2\xi_0^{64} + 4\xi_0^{72}\right] \\ &+ \xi_2^2\left[2\xi_1^{24}\xi_0 + 5\xi_1^{22}\xi_0^9 + 2\xi_1^{12}\xi_0^{49} + 3\xi_1^{10}\xi_0^{57} + 2\xi_1^8\xi_0^{65}\right] \\ &+ \xi_2\left[6\xi_1^{30}\xi_0^2 + \xi_1^{28}\xi_0^{10} + 5\xi_1^{18}\xi_0^{50} + 4\xi_1^{16}\xi_0^{58} + 5\xi_1^{14}\xi_0^{66}\right] \\ &\qquad + \xi_2\left[+6\xi_1^6\xi_0^{98} + 3\xi_1^4\xi_0^{106} + 4\xi_1^2\xi_0^{114} + \xi_0^{122}\right] \\ &+ \left[6\xi_1^{36}\xi_0^3 + 4\xi_1^{24}\xi_0^{51} + 2\xi_1^{22}\xi_0^{59} + 4\xi_1^{12}\xi_0^{99} + 3\xi_1^{10}\xi_0^{107} + 6\xi_1^8\xi_0^{115}\right]\end{aligned}$$

- $q = 9$

$$\begin{aligned}\phi_2 &= \xi_2^7\left[2\xi_1^2\xi_0^{27} + \xi_0^{37}\right] + \xi_2^6\left[\xi_1^{12}\xi_0^{18} + \xi_1^{10}\xi_0^{28}\right] + \xi_2^4\left[2\xi_1^{32} + \xi_1^{30}\xi_0^{10}\right] \\ &+ \xi_2^3\left[2\xi_1^{40}\xi_0 + \xi_1^{36}\xi_0^{21} + 2\xi_1^{24}\xi_0^{81} + \xi_1^{18}\xi_0^{111} + 2\xi_1^6\xi_0^{171} + \xi_0^{201}\right] \\ &+ \xi_2\left[2\xi_1^{56}\xi_0^3 + \xi_1^{54}\xi_0^{13} + 2\xi_1^8\xi_0^{243} + \xi_1^6\xi_0^{253} + \xi_1^2\xi_0^{273} + 2\xi_0^{283}\right] \\ &+ \left[2\xi_1^{64}\xi_0^4 + 2\xi_1^{48}\xi_0^{84} + 2\xi_1^{30}\xi_0^{174} + 2\xi_1^{16}\xi_0^{244} + 2\xi_1^{12}\xi_0^{264} + \xi_1^{10}\xi_0^{274}\right]\end{aligned}$$

Considering each ϕ_2 as a polynomial in ξ_2 we can make the following generalisations.

- The coefficient of ξ_2^{q-2}, the largest degree of ξ_2 is

$$\pm \frac{(q-1)}{2}\left(\xi_1^2 - \xi_0^{q+1}\right)(\xi_0^q)^{\frac{q-3}{2}}$$

or

$$\pm d\Lambda_2(\xi_0^q)^{d-1}$$

where

$$\Lambda_2 = \xi_1^2 - \xi_0^{q+1} \quad \text{and given} \quad d = \frac{q-1}{2}.$$

This choice of notation for $\xi_1^2 - \xi_0^{q+1}$ conforms to the notation of Chapter 5.

- The coefficient of ξ_2^{q-3} is

$$\left(\xi_1^2 - \xi_0^{q+1}\right)\xi_1^{q+1}(\xi_0^q)^{\frac{q-5}{2}} = \Lambda_2\xi_1^{q+1}(\xi_0^q)^{d-2}$$

- The coefficient of ξ_2 is

$$(\xi_1^2 - \xi_0^{q+1})\left(\left((\xi_1^2 - \xi_0^{q+1})^q + \xi_1^2\xi_0^{q^2-1}\right)\xi_0\right)^{d-1}$$

or

$$\Lambda_2\left((\Lambda_2^q + B)\xi_0\right)^{d-1} \quad \text{where} \quad B = \xi_1^2\xi_0^{q^2-1}$$

- Terms in which the degree of ξ_2 is zero are of the form

$$\pm \frac{\xi_0^{\frac{q-1}{2}}\xi_1^{q+1}\left(\left((\xi_1^2 - \xi_0^{q+1})^q + \xi_1^2\xi_0^{q^2-1}\right)^{\frac{q-1}{2}} - \left(\xi_1^2\xi_0^{q^2-1}\right)^{\frac{q-1}{2}}\right)}{(\xi_1^2 - \xi_0^{q+1})^q}$$

or

$$\pm \frac{\xi_0^d\xi_1^{q+1}\left((\Lambda_2^q + B)^d - B^d\right)}{\Lambda_2^q}$$

The invariants d_2 are given in Appendix B.1.

4.5 The ring of invariants of $O(3, q)$

We have seen that in the case for n odd there is one Orthogonal group $O(n, q)$ up to isomorphism. The ring of invariants of this group was presented by Cohen S.D. in the following theorem and an alternative proof given by Larry Smith in [19].

Theorem 4.3 ((SD Cohen): [19]). *If $q = p^v$, where p is an odd prime, then*

$$\mathbb{F}_q[x, y, z]^{O(3,\mathbb{F}_q)} = \mathbb{F}_q[Q, P^{\Delta_1}(Q), E]$$

where $Q = y^2 - xz$, $\deg(P^{\Delta_1}(Q)) = q + 1$ and $\deg(E) = q(q - 1)$.

On the basis of this theorem we present the following conjecture.

Conjecture 4.4. Let ξ_0 be the non-singular quadratic form in the 3 variables x_1, x_2, x_3 over the finite field $\mathbb{F}_q$ and the form ξ_1 be determined from ξ_0 as described in §3.2. Then let the polynomial d_2 be as defined in the statement of Conjecture 4.1. The ring of invariants of the Orthogonal group $O(\xi_0)$ is then

$$\mathbb{F}_q[x_1, x_2, x_3]^{O(\xi_0)} = \mathbb{F}_q[\xi_0, \xi_1, d_2]$$

We note that the degrees of the generators of the ring $\mathbb{F}_q[\xi_0, \xi_1, d_2]$ are equal to those of the ring $\mathbb{F}_q[Q, P^{\Delta_1}(Q), E]$ as Q and ξ_0 are quadratic forms, the degree of ξ_1 is $q + 1$ by definition and the degree of d_2 is equal to that of the qth root of the Dickson invariant $c_{3,2}$ which is $\frac{q^3-q^2}{q} = q(q - 1)$.

In addition we note that Conjecture 4.4 is consistent with [8]: Theorem C in terms of the degrees of the proposed generators of the Orthogonal group.

4.6 The ϕ_i and d_i polynomials in the case $n = 4$

The CoCoA code for the case when $n = 4$ and $q = 3$ with $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is given in Appendix B.2 with the output in Appendix B.3 giving the ϕ_i polynomials. The code in Appendix B.4 calculates the d_i invariants from d_i^q. We have used the code to calculate each of the invariants d_i for $i = 1, \ldots, 3$ in this case as these are used in explicit calculations in later sections. The resulting d_i polynomials are then given implicitly in the following definition.

Definition 4.5. When $n = 4$ and $q = 3$ with $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ we define the d_i polynomials implicitly in the following equations:

$$\begin{aligned} d_3^q &= c_3 + \xi_0\xi_1^{13} - \xi_0^4\xi_1^9\xi_2 - \xi_0^{10}\xi_1\xi_2^3 + \xi_0^{13}\xi_3 + \xi_1^{11}\xi_2 - \xi_0^9\xi_1^2\xi_3 + \xi_0\xi_1^3\xi_2^4 - \xi_0\xi_1^6\xi_3 \\ &\quad + \xi_1\xi_2^5 - \xi_1^4\xi_2\xi_3 - \xi_0^3\xi_2^2\xi_3 \end{aligned}$$

$$\begin{aligned} d_2^q &= c_2 - \xi_0^{28}\xi_1^4 + \xi_0^{31}\xi_2 - \xi_0^{27}\xi_1^2\xi_2 + \xi_0\xi_1^{10}\xi_2^3 - \xi_0^4\xi_1^9\xi_3 + \xi_1^{11}\xi_3 - \xi_0\xi_2^7 + \xi_0\xi_1^3\xi_2^3\xi_3 \\ &\quad - \xi_1\xi_2^4\xi_3 + \xi_1^4\xi_3^2 - \xi_0^3\xi_2\xi_3^2, \end{aligned}$$

$$\begin{aligned} d_1^q &= c_1 + \xi_0^{37}\xi_1 - \xi_0^{28}\xi_1^3\xi_2 - \xi_0^{27}\xi_1\xi_2^2 - \xi_0\xi_1^{19} + \xi_0\xi_1^9\xi_2^4 + \xi_0\xi_1^{12}\xi_3 - \xi_0^{10}\xi_2^3\xi_3 - \xi_1^{10}\xi_2\xi_3 \\ &\quad - \xi_0^9\xi_1\xi_3^2 + \xi_2^5\xi_3 + \xi_1^3\xi_2\xi_3^2 \end{aligned}$$

Chapter 5

The Λ_k invariants

In this chapter we work initially in the polynomial ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and define the polynomial Λ_n in the forms $\xi_0, \xi_1, \xi_2, \ldots$ defined in §3.2. As we have seen in §3.2 each form ξ_j is determined by the choice of ξ_0 through the action of the Steenrod algebra and so is an invariant of the Orthogonal group $O(\xi_0)$. We then generalise the definition of Λ_n to define the polynomials l_k in the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$. In §5.2 we show that each polynomial l_k for $k \geq 2$ is the product of two non trivial irreducible polynomials l_k^+ and l_k^- in the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$.

In §5.4 we consider the image of the polynomials l_k, l_k^+ and l_k^- under the ring homomorphism from the polynomial ring $\mathbb{F}_q[s_0, s_1, \ldots, s_n]$ to $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ defined by fixing the image of s_i as ξ_i and thus induced by the choice of quadratic form ξ_0. We note that the images Λ_k, Λ_k^+ and Λ_k^- of l_k, l_k^+ and l_k^- respectively under this map are each invariants of the Orthogonal group $O(\xi_0)$. We then consider the factorisation of the invariants Λ_k^+ and Λ_k^- over the ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

5.1 The l_k polynomials

We work with the general quadratic form

$$\xi_0 = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2$$

and define the associated diagonal matrix

$$B = \begin{pmatrix} \varepsilon & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

In Section 3.1 we defined the Dickson matrix $D_n(X)$ with determinant $\Delta_n(X)$ in the proof of Lemma 3.1 and in the statement of Lemma 3.4 we defined $\ell = \Delta_{n-1}(x_n)$. We now define the matrix

$$L = D_{n-1}(x_n)$$

and note that $\det(L) = \ell$. Thus

$$L = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_1^q & x_2^q & \dots & x_n^q \\ x_1^{q^2} & x_2^{q^2} & \dots & x_n^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \dots & x_n^{q^{n-1}} \end{pmatrix}.$$

Definition 5.1. Denote by Λ_n the determinant of the matrix LBL^T where the matrices L and B are defined above.

Thus it can be seen that

$$\Lambda_n = \begin{vmatrix} \xi_0 & \xi_1 & \xi_2 & \xi_3 & \dots & \xi_{n-1} \\ \xi_1 & \xi_0^q & \xi_1^q & \xi_2^q & \dots & \xi_{n-2}^q \\ \xi_2 & \xi_1^q & \xi_0^{q^2} & \xi_1^{q^2} & \dots & \xi_{n-3}^{q^2} \\ \xi_3 & \xi_2^q & \xi_1^{q^2} & \xi_0^{q^3} & \dots & \xi_{n-4}^{q^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{n-1} & \xi_{n-2}^q & \xi_{n-3}^{q^2} & \xi_{n-4}^{q^3} & \dots & \xi_0^{q^{n-1}} \end{vmatrix}$$

in the notation of Section 3.2 and that

$$\Lambda_n = \varepsilon \ell^2.$$

Definition 5.2. Working in the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \dots]$, define for each $k \geq 1$

$$\mathcal{L}_k = \begin{pmatrix} s_0 & s_1 & s_2 & s_3 & \dots & s_{k-1} \\ s_1 & s_0^q & s_1^q & s_2^q & \dots & s_{k-2}^q \\ s_2 & s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-3}^{q^2} \\ s_3 & s_2^q & s_1^{q^2} & s_0^{q^3} & \dots & s_{k-4}^{q^3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-1} & s_{k-2}^q & s_{k-3}^{q^2} & s_{k-4}^{q^3} & \dots & s_0^{q^{k-1}} \end{pmatrix}$$

and define the polynomials

$$l_k = \det \mathcal{L}_k.$$

We also define

$$l_0 = 1.$$

5.2 The polynomials l_k^+ and l_k^-

We wish to prove that each l_k of Definition 5.2 is the product of two non trivial irreducible polynomials l_k^+ and l_k^- over $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ for $k \geq 2$.

Definition 5.3. We define

$$l_0^+ = 1 \qquad \text{and} \qquad l_0^- = 1$$
$$l_1^+ = 1 \qquad \text{and} \qquad l_1^- = s_0$$

Thus by definition we see that $l_k = l_k^+ l_k^-$ in the cases when $k = 0, 1$.

In the case when $k = 2$ we see that

$$\begin{aligned} l_2 &= s_0^{q+1} - s_1^2 \\ &= (s_0^{\frac{q+1}{2}} + s_1)(s_0^{\frac{q+1}{2}} - s_1) \end{aligned}$$

We define

$$l_2^+ = s_0^{\frac{q+1}{2}} + s_1 \quad \text{and} \quad l_2^- = s_0^{\frac{q+1}{2}} - s_1$$

Thus we see that l_2 is the product of the two irreducible polynomials l_2^+ and l_2^-.

Before considering l_k for $k = 3, 4, \dots$ we present two Lemmas concerning the determinant and minors of a given square matrix.

Lemma 5.4 (Sylvester: [11] Lemma 2 of Chapter 8)**.** *For any d by d matrices A and B and $1 \leq c \leq d$*

$$\det(A) \cdot \det(B) = \sum \det(A') \cdot \det(B')$$

where the sum is taken over all pairs (A', B') of matrices obtained from A and B by interchanging a fixed set of c columns of B with any set of c columns of A, preserving order.

Lemma 5.5. *Let $k \geq 3$ and let M be a k by k matrix and $\check{M}$ the 'middle' minor of M, that is the determinant of the sub matrix of M with the 1st and kth rows and the 1st and kth columns removed.*

Then

$$\check{M} \cdot det(M) = M_{k,k}M_{1,1} - M_{k,1}M_{1,k}$$

where $M_{i,j}$ is the minor of M with the ith row and jth column deleted.

We have seen that this conjecture is true for any d by d matrix for $d = 1, .., 8$ by calculation using CoCoA code. The code is given in Appendix C.1 together with the output.

Proof. Let

$$M = \begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,k} \\ m_{2,1} & m_{2,2} & \dots & m_{2,k} \\ \vdots & \vdots & \ddots & \dots \\ m_{k,1} & m_{k,2} & \dots & m_{k,k} \end{pmatrix} \quad \text{so that} \quad \check{M} = \begin{vmatrix} m_{2,2} & \dots & m_{2,k-1} \\ \vdots & \ddots & \dots \\ m_{k-1,2} & \dots & m_{k-1,k-1} \end{vmatrix}.$$

We denote by $\overline{M}$ the matrix M with the 1st and kth rows removed and by $\check{M}_{i,j}$ for $1 \leq i, j \leq k$ with $i \neq j$ the minor of M that is the determinant of the $k-2$ by $k-2$ sub matrix of M that is the matrix $\overline{M}$ with the ith and jth columns removed. Thus

$$\check{M}_{i,j} = \begin{pmatrix} m_{2,1} & \dots & m_{2,i-1} & m_{2,i+1} & \dots & m_{2,j-1} & m_{2,j+1} & \dots & m_{2,k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{k-1,1} & \dots & m_{k-1,i-1} & m_{k-1,i+1} & \dots & m_{k-1,j-1} & m_{k-1,j+1} & \dots & m_{k-1,k} \end{pmatrix}.$$

If $i = j$ let $\check{M}_{i,j} = 0$.

With this notation we have

$$\begin{aligned}\det(M) &= \sum_{i=1}^{k}\sum_{j=1}^{k}(-1)^{i+j+k+1}\, m_{1,i}\, m_{k,j}\, \check{M}_{i,j} \\ &= \sum_{i=1}^{k-1}\sum_{j=i+1}^{k}(-1)^{i+j+k+1}\,(m_{1,i}m_{k,j} - m_{1,j}mk,i)\check{M}_{i,j} \quad ,\end{aligned}$$

$$\check{M} = \check{M}_{1,k} \qquad \text{and}$$

$$M_{1,1} = \sum_{i=2}^{k}(-1)^{i+k}m_{k,i}\check{M}_{1,i}, \qquad M_{1,k} = \sum_{i=1}^{k-1}(-1)^{i+k+1}m_{k,i}\check{M}_{i,k},$$

$$M_{k,1} = \sum_{i=2}^{k}(-1)^{i}m_{1,i}\check{M}_{1,i} \quad \text{and} \quad M_{k,k} = \sum_{i=1}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k}.$$

Now we have $M_{k,k}M_{1,1} - M_{k,1}M_{1,k}=$

$$\begin{aligned}&\sum_{i=1}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k}\ \sum_{i=2}^{k}(-1)^{i+k}m_{k,i}\check{M}_{1,i} \\ &\qquad -\sum_{i=2}^{k}(-1)^{i}m_{1,i}\check{M}_{1,i}\ \sum_{i=1}^{k-1}(-1)^{i+k+1}m_{k,i}\check{M}_{i,k} \\ = &\left[m_{1,1}\check{M} + \sum_{i=2}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k}\right]\left[m_{k,k}\check{M} + \sum_{i=2}^{k-1}(-1)^{i+k}m_{k,i}\check{M}_{1,i}\right] \\ &-\left[(-1)^{k}m_{1,k}\check{M} + \sum_{i=2}^{k-1}(-1)^{i}m_{1,i}\check{M}_{1,i}\right]\left[(-1)^{k}m_{k,1}\check{M} + \sum_{i=2}^{k-1}(-1)^{i+k+1}m_{k,i}\check{M}_{i,k}\right] \\ = &\ \check{M}\left[m_{1,1}m_{k,k}\check{M} + m_{k,k}\sum_{i=2}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k} + m_{1,1}\sum_{i=2}^{k-1}(-1)^{i+k}m_{k,i}\check{M}_{1,i}\right] \\ &-\check{M}\left[m_{1,k}m_{k,1}\check{M} + m_{k,1}\sum_{i=2}^{k-1}(-1)^{i+k}m_{1,i}\check{M}_{1,i} + m_{1,k}\sum_{i=2}^{k-1}(-1)^{i+1}m_{k,i}\check{M}_{i,k}\right] \\ &+\sum_{i=2}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k}\sum_{i=2}^{k-1}(-1)^{i+k}m_{k,i}\check{M}_{1,i} - \sum_{i=2}^{k-1}(-1)^{i}m_{1,i}\check{M}_{1,i}\sum_{i=2}^{k-1}(-1)^{i+k+1}m_{k,i}\check{M}_{i,k}.\end{aligned}$$

Thus we have $M_{k,k}M_{1,1} - M_{k,1}M_{1,k}$

$$\begin{aligned} = \quad & \check{M}\left[m_{1,1}m_{k,k}\check{M} + m_{k,k}\sum_{i=2}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k} + m_{1,1}\sum_{i=2}^{k-1}(-1)^{i+k}m_{k,i}\check{M}_{1,i}\right] \\ & -\check{M}\left[m_{1,k}m_{k,1}\check{M} + m_{k,1}\sum_{i=2}^{k-1}(-1)^{i+k}m_{1,i}\check{M}_{1,i} + m_{1,k}\sum_{i=2}^{k-1}(-1)^{i+1}m_{k,i}\check{M}_{i,k}\right] \\ & + \sum_{i,j=2}^{k-1}(-1)^{i+j+k+1}m_{1,i}m_{k,j}\left(\check{M}_{1,j}\check{M}_{i,k} - \check{M}_{1,i}\check{M}_{j,k}\right) \end{aligned}$$

Now for each $1 < i < j < k$ we need to prove that

$$\check{M}_{1,j}\check{M}_{i,k} - \check{M}_{1,i}\check{M}_{j,k} = \check{M}_{1,k}\check{M}_{i,j}. \tag{5.1}$$

With reference to Lemma 5.4 we set $A = \check{M}_{1,k}$ and $B = \check{M}_{i,j}$ so that $d = k - 2$. Then we set $c = 1$ and take the fixed set of c columns of the matrix B to be the first column of B.

Denoting by $\check{m}_l$ the lth column of the matrix $\overline{M}$ defined in the statement of this Lemma we note that the fixed column of N set above is $\check{m}_1$. We then proceed to consider interchanging this column with any column of the matrix $A = \check{M}_{1,k}$.

Now on interchanging $\check{m}_l$ of matrix A with $\check{m}_1$ of matrix B for each $1 < l < k$ and $l \neq i, j$ to produce the matrices A' and B' we note that B' will have two identical columns so that $\det(B') = 0$. Thus we see that

$$\det(A) \cdot \det(B) = \det(A^{i,1}) \cdot \det(B^{1,i}) + \det(A^{j,1}) \cdot \det(B^{1,j})$$

where $A^{e,1}$ and $B^{1,e}$ denote, for $1 < e < k$, the matrices A and B with the $(e-1)$th column of A interchanged with the 1st column of B that is interchanging the column $\check{m}_e$ of matrix A with the column $\check{m}_1$ of matrix B.

Considering the reordering of the columns of the matrices we note that

$$\det(A^{i,1}) = (-1)^{i-2}\check{M}_{i,k}, \quad \text{and} \quad \det(B^{1,i}) = (-1)^{i-2}\check{M}_{1,j}$$

and that

$$\det(A^{j,1}) = (-1)^{j-2}\check{M}_{j,k} \quad \text{and} \quad \det(B^{1,j}) = (-1)^{j-1}\check{M}_{1,i}.$$

Thus we see that $\det(A^{i,1}) \cdot \det(B^{1,i}) = \check{M}_{i,k}\check{M}_{1,j}$ and $\det(A^{j,1}) \cdot \det(B^{1,j}) = -\check{M}_{j,k}\check{M}_{1,i}$ so that Equation 5.1 is true as required.

Hence $M_{k,k}M_{1,1} - M_{k,1}M_{1,k}$

$$\begin{aligned}
&= \check{M}\left[m_{1,1}m_{k,k}\check{M} + m_{k,k}\sum_{i=2}^{k-1}(-1)^{i+1}m_{1,i}\check{M}_{i,k} + m_{1,1}\sum_{i=2}^{k-1}(-1)^{i+k}m_{k,i}\check{M}_{1,i}\right] \\
&\quad -\check{M}\left[m_{1,k}m_{k,1}\check{M} + m_{k,1}\sum_{i=2}^{k-1}(-1)^{i+k}m_{1,i}\check{M}_{1,i} + m_{1,k}\sum_{i=2}^{k-1}(-1)^{i+1}m_{k,i}\check{M}_{i,k}\right] \\
&\quad +\check{M}\sum_{i,j=2}^{k-1}(-1)^{i+j+k+1}m_{1,i}m_{k,j}\check{M}_{i,j} \\
&= \check{M}\sum_{i,j=1}^{k}(-1)^{i+j+k+1}\ m_{1,i}\ m_{k,j}\ \check{M}_{i,j} \\
&= \check{M}\cdot det(M)
\end{aligned}$$

as required. □

Lemma 5.6. *Let l_{k+1} be the polynomial as defined in Definition 5.2. Then*

$$l_{k+1} = \frac{\left((l_k)^{q+1} - w_k^2\right)}{(l_{k-1})^q}$$

where

$$w_k = \begin{vmatrix}
s_1 & s_2 & s_3 & \dots & s_{k-1} & s_k \\
s_0^q & s_1^q & s_2^q & \dots & s_{k-2}^q & s_{k-1}^q \\
s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-3}^{q^2} & s_{k-2}^{q^2} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
s_{k-2}^q & s_{k-3}^{q^2} & s_{k-4}^{q^3} & \dots & s_0^{q^{k-1}} & s_1^{q^{k-1}}
\end{vmatrix},$$

that is w_k is the determinant of the matrix $\mathcal{L}_{k+1}$ given in Definition 5.2 with the $(k+1)$th row and 1st column removed.

Proof. In the identity of Lemma 5.5 we set matrix $M = \mathcal{L}_{k+1}$ of Definition 5.2.

Then

$$\det(M) = l_{k+1},$$

$$\check{M} = (l_{k-1})^q, \quad M_{k,k} = l_k, \quad M_{1,1} = (l_k)^q$$

and

$$M_{k,1} = M_{1,k} = w_k.$$

Thus we have

$$l_{k+1}(l_{k-1})^q = l_k(l_k)^q - (w_k)^2.$$

The result follows. □

Lemma 5.7. *The polynomial l_k factorises non trivially over the ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-1}]$ for $k \geq 2$. In particular l_k factorises as the product of two factors each linear in s_{k-1}.*

Proof. From Lemma 5.6 we have

$$l_{k+1} = \frac{\left(l_k^{q+1} - w_k^2\right)}{(l_{k-1})^q}$$

Thus

$$l_k = \frac{\left(l_{k-1}^{\frac{q+1}{2}} + w_{k-1}\right)\left(l_{k-1}^{\frac{q+1}{2}} - w_{k-1}\right)}{(l_{k-2})^q}$$

Let

$$f_k^+ = l_{k-1}^{\frac{q+1}{2}} + w_{k-1}, \qquad f_k^- = l_{k-1}^{\frac{q+1}{2}} - w_{k-1} \quad \text{and} \quad \lambda = (l_{k-2})^q$$

Now l_k is a polynomial in the Unique Factorisation Domain $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-1}]$ and so each irreducible factor of λ must divide one of f_k^+ or f_k^-. We consider each of f_k^+, f_k^- and λ as polynomials in s_{k-1} with coefficients in $\mathbb{F}_q[s_0, s_1, \ldots, s_{k-2}]$. By definition w_{k-1} is linear in s_{k-1} and l_{k-1} has no terms in s_{k-1}. It follows that both f_k^+ and f_k^- are linear in s_{k-1}. Thus let $f_k^+ = a_1 s_{k-1} + b_1$ and $f_k^- = a_2 s_{k-1} + b_2$, where a_1, b_1, a_2, b_2 are polynomials in $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-2}]$.

By definition l_{k-2} has no term in s_{k-1} and so we can let $\lambda = \lambda_1\lambda_2 \ldots \lambda_r\lambda_{r+1} \ldots \lambda_s$ where each λ_i is an irreducible polynomial in $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-2}]$ such that each $\lambda_i | f_k^+$ for $i = 1, 2, \ldots, r$ and that $\lambda_i | f_k^-$ for $i = r+1, \ldots, s$ without loss of generality.

Now we can divide $f_k^+ = a_1 s_{k-1} + b_1$ through by λ_1 noting that $\lambda_1 | a_1$ and $\lambda_1 | b_1$ so that

$$\frac{f_k^+}{\lambda_1} = a_1' s_{k-1} + b_1'$$

for some $a_1', b_1' \in \mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-2}]$. Continuing thus with the factors $\lambda_2, \ldots, \lambda_r$ we have

$$l_k = l_k^+ \frac{f_k^-}{\lambda_{r+1} \ldots \lambda_s}$$

where $l_k^+ = a_1^{(r)} s_{k-1} + b_1^{(r)}$ for some $a_1^{(r)}, b_1^{(r)} \in \mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-2}]$.

Similarly we can divide $f_k^- = a_2 s_{k-1} + b_2$ through by λ_i for $i = r+1, \ldots, s$ so that

$$l_k = l_k^+ \, l_k^- \tag{5.2}$$

where $l_k^- = a_2^{(s)} s_{k-1} + b_2^{(s)}$ for some $a_2^{(r)}, b_2^{(r)} \in \mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-2}]$.

Each of $a_1^{(r)} s_{k-1} + b_1^{(r)}$ and $a_2^{(s)} s_{k-1} + b_2^{(s)}$ is a non trivial polynomial in $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-1}]$ and thus we see that l_k factorises non trivially. In particular we see that each of the factors l_k^+ and l_k^- of l_k are linear in s_{k-1} as required. □

Definition 5.8. We denote by l_k^+ and l_k^- the non trivial factors of l_k that are linear in s_{k-1} so that

$$l_k = l_k^+ l_k^-.$$

Lemma 5.9. *The polynomials l_k and w_k are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ for $k \geq 1$ where l_k is given in Definition 5.2 and w_k is defined in the statement of Lemma 5.6.*

Proof. Recall that

$$l_k = \begin{vmatrix} s_0 & s_1 & s_2 & \ldots & s_{k-1} \\ s_1 & s_0^q & s_1^q & \ldots & s_{k-2}^q \\ s_2 & s_1^q & s_0^{q^2} & \ldots & s_{k-3}^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-1} & s_{k-2}^q & s_{k-3}^{q^2} & \ldots & s_0^{q^{k-1}} \end{vmatrix} \text{ and } w_k = \begin{vmatrix} s_1 & s_2 & s_3 & \ldots & s_k \\ s_0^q & s_1^q & s_2^q & \ldots & s_{k-1}^q \\ s_1^q & s_0^{q^2} & s_1^{q^2} & \ldots & s_{k-2}^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-2}^q & s_{k-3}^{q^2} & s_{k-4}^{q^3} & \ldots & s_1^{q^{k-1}} \end{vmatrix}.$$

We aim to prove the statement that w_k and l_k are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ for $k \geq 1$ by induction on k.

To start, letting $k = 1$, we have

$$l_1 = s_0 \text{ and } w_1 = s_1.$$

and so we see that l_1 and w_1 are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ and thus have the basis for the induction.

Now assume that the statement is true when $k = m$ that is that l_m and w_m are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$. We wish to deduce that l_{m+1} and w_{m+1} are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ and assume to the contrary that l_{m+1} and w_{m+1} are not coprime and so have a common factor, say f, that can be assumed to be an irreducible polynomial in in $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$.

We have by definition that

$$w_{m+1} = -(l_m)^q s_{m+1} + \text{ terms not involving } s_{m+1}.$$

Thus any factor of w_{m+1} must divide $(l_m)^q$ so that

$$f|(l_m)^q \quad \text{and so} \quad f|(l_m)^{q+1}.$$

Now

$$l_{m+1} = \frac{(l_m)^{q+1} - w_m^2}{l_{m-1}^q}$$

by Lemma 5.6 and by assumption $f|l_{m+1}$ so that $f|l_{m+1} \cdot (l_{m-1})^q = (l_m)^{q+1} - w_m^2$.

We have seen above that $f|(l_m)^{q+1}$ and so it follows that $f|w_m^2$. Thus, as f is irreducible, we see that f divides both w_m and l_m which contradicts the inductive hypothesis. Therefore l_{m+1} and w_{m+1} are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ if l_m and w_m are coprime and so as l_1 and w_1 are coprime we conclude that l_k and w_k are coprime in $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ for all $k \geq 1$.

□

We now wish to determine inductive formulae to generate l_k^+ and l_k^- for $k \geq 3$. Having that

$$l_k = \frac{(l_{k-1})^{q+1} - w_{k-1}^2}{(l_{k-2})^q} = \frac{\left((l_{k-1})^{\frac{q+1}{2}} + w_{k-1}\right)\left((l_{k-1})^{\frac{q+1}{2}} - w_{k-1}\right)}{(l_{k-2})^q}$$

we need to ascertain which factors of $(l_{k-2})^q$ divide each of the expressions $l_{k-1}^{\frac{q+1}{2}} \pm w_{k-1}$, noting that each must divide one or other as l_k is a polynomial.

CoCoA code was written to determine this in the cases $q = 3$ and $q = 5$ for small values of k. It was found that $(l_{k-2}^{\pm})^q$ divides $(l_{k-1})^{\frac{q+1}{2}} \pm w_{k-1}$ when $q = 3$ and that $(l_{k-2}^{\mp})^q$ divides $(l_{k-1})^{\frac{q+1}{2}} \pm w_{k-1}$ when $q = 5$.

Thus an algorithm to generate the $l_k^{\pm}$ inductively was formulated and implemented with CoCoA code. This code is given in Appendix C.2.1 for the case $n = 4$ and $l_k^{\pm}$. The output from the code is given in Appendix C.3 for $q = 3$ and $q = 5$.

The results obtained using code were then generalized in Theorem 5.11. Before stating and proving the theorem we establish the coefficients of s_{k-1}^2 in the expressions $(l_k)^{\frac{q+1}{2}} \pm w_k$ for $k \geq 2$.

Lemma 5.10. *The coefficient of* $(s_{k-1})^{q+1}$ *in* $(l_k)^{\frac{q+1}{2}} \pm w_k$ *is*

$$\left[(l_{k-2})^{\frac{q+1}{2}} \pm w_{k-2}\right]^q \quad \textit{when } q \equiv 3 \bmod 4 \quad \textit{and} \quad -\left[(l_{k-2})^{\frac{q+1}{2}} \mp w_{k-2})\right]^q \quad \textit{when } q \equiv 1 \bmod 4.$$

Proof. By definition 5.2 the coefficient of $(s_{k-1})^2$ in l_k is

$$(-1)^k(-1)^{k-1}\begin{vmatrix} s_0^q & s_1^q & s_2^q & \dots & s_{k-3}^q \\ s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-4}^{q^2} \\ s_2^q & s_1^{q^2} & s_0^{q^3} & \dots & s_{k-5}^{q^3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-3}^q & s_{k-4}^{q^2} & s_{k-5}^{q^3} & \dots & s_0^{q^{k-3}} \end{vmatrix} = -(l_{k-2})^q$$

by definition and the Frobenius map.

Thus the coefficient of $(s_{k-1})^{q+1}$ in $(l_k)^{\frac{q+1}{2}}$ is $((-l_{k-2})^q)^{\frac{q+1}{2}} = (l_{k-2})^{\frac{q(q+1)}{2}}$ when $q \equiv 3 \bmod 4$ as then $\frac{q+1}{2}$ is even and $-(l_{k-2})^{\frac{q(q+1)}{2}}$ when $q \equiv 1 \bmod 4$ as then $\frac{q+1}{2}$ is odd.

By the definition given in the statement of Lemma 5.6 the coefficient of $(s_{k-1})^{q+1}$ in w_k is equal to

$$(-1)^k(-1)^{k-2}\begin{vmatrix} s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-4}^{q^2} \\ s_2^q & s_1^{q^2} & s_0^{q^3} & \dots & s_{k-5}^{q^3} \\ s_3^q & s_2^{q^2} & s_1^{q^3} & \dots & s_{k-6}^{q^4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-2}^q & s_{k-3}^{q^2} & s_{k-4}^{q^3} & \dots & s_1^{q^{k-2}} \end{vmatrix}$$

and so to

$$\left|\begin{pmatrix} s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-4}^{q^2} \\ s_2^q & s_1^{q^2} & s_0^{q^3} & \dots & s_{k-5}^{q^3} \\ s_3^q & s_2^{q^2} & s_1^{q^3} & \dots & s_{k-6}^{q^4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-2}^q & s_{k-3}^{q^2} & s_{k-4}^{q^3} & \dots & s_1^{q^{k-2}} \end{pmatrix}^T\right| = \begin{vmatrix} s_1^q & s_2^q & s_3^q & \dots & s_{k-2}^q \\ s_0^{q^2} & s_1^{q^2} & s_2^{q^2} & \dots & s_{k-3}^{q^2} \\ s_1^{q^2} & s_0^{q^3} & s_1^{q^3} & \dots & s_{k-4}^{q^3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-4}^{q^2} & s_{k-5}^{q^3} & s_{k-6}^{q^4} & \dots & s_1^{q^{k-2}} \end{vmatrix}$$

and thus to

$$\begin{vmatrix} s_1 & s_2 & s_3 & \dots & s_{k-2} \\ s_0^q & s_1^q & s_2^q & \dots & s_{k-3}^q \\ s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-4}^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-4}^q & s_{k-5}^{q^2} & s_{k-6}^{q^3} & \dots & s_1^{q^{k-3}} \end{vmatrix}^q$$

by the Frobenius map.

Thus the coefficient of $(s_{k-1})^{q+1}$ in w_k is equal to $(w_{k-2})^q$.

Then the coefficient of $(s_{k-1})^{q+1}$ in $l_k^{\frac{q+1}{2}} \pm w_k$ is

$$(l_{k-2})^{\frac{q(q+1)}{2}} \pm (w_{k-2})^q = \left[(l_{k-2})^{\frac{q+1}{2}} \pm w_{k-2}\right]^q \text{ when } q \equiv 3 \bmod 4 \text{ and}$$

$$-(l_{k-2})^{\frac{q(q+1)}{2}} \pm (w_{k-2})^q = -\left[(l_{k-2})^{\frac{q+1}{2}} \mp w_{k-2})\right]^q \text{ when } q \equiv 1 \bmod 4$$

as required. □

Theorem 5.11. *The polynomial l_k for $k \geq 2$ factorises over the ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-1}]$ as the product of the two irreducible polynomials l_k^+ and l_k^- defined inductively below for $k \geq 3$.*

When $q \equiv 3 \mod 4$

$$l_k^+ = \frac{(l_{k-1})^{\frac{q+1}{2}} + w_{k-1}}{(l_{k-2}^+)^q} \qquad l_k^- = \frac{(l_{k-1})^{\frac{q+1}{2}} - w_{k-1}}{(l_{k-2}^-)^q}$$

and when $q \equiv 1 \mod 4$

$$l_k^+ = \frac{(l_{k-1})^{\frac{q+1}{2}} + w_{k-1}}{(l_{k-2}^-)^q} \qquad l_k^- = \frac{(l_{k-1})^{\frac{q+1}{2}} - w_{k-1}}{(l_{k-2}^+)^q}.$$

Proof. Applying Lemma 5.6 to l_k we have

$$l_k = \frac{(l_{k-1})^{q+1} - w_{k-1}^2}{(l_{k-2})^q}$$

and on factorisation of the numerator

$$l_k = \frac{\left((l_{k-1})^{\frac{q+1}{2}} + w_{k-1}\right)\left((l_{k-1})^{\frac{q+1}{2}} - w_{k-1}\right)}{(l_{k-2})^q}.$$

We note that each of the the irreducible factors of $(l_{k-2})^q$ must divide one of the expressions $(l_k)^{\frac{q+1}{2}} + w_k$ or $(l_k)^{\frac{q+1}{2}} - w_k$ exactly in the Unique Factorisation Domain $\mathbb{F}_q[s_0, s_1, s_2, \ldots, s_{k-1}]$.

We recall from Definition 5.3 that

$$l_1^+ = 1 \text{ and } l_1^- = s_0$$

and that

$$l_2^+ = s_0^{\frac{q+1}{2}} + s_1 \text{ and } l_1^- = s_0^{\frac{q+1}{2}} - s_1$$

and note that the polynomials l_2^+ and l_2^- are both irreducible and are not associates.

We now consider the cases when $q = 3 \mod 4$ and when $q = 1 \mod 4$ separately.

(i) Let $q = 3 \mod 4$ and note that $\frac{q+1}{2}$ is even.

Then let P_k be the statement that l_k factorises as the product of two irreducible polynomials l_k^+ and l_k^- that are not associates such that

$$l_k^+ = \frac{l_{k-1}^{\frac{q+1}{2}} + w_{k-1}}{(l_{k-2}^+)^q} \qquad l_k^- = \frac{l_{k-1}^{\frac{q+1}{2}} - w_{k-1}}{(l_{k-2}^-)^q}. \tag{5.3}$$

We prove that P_k is true for $k \geq 3$ by induction in steps of 2 as we are concerned with dividing by the factors of $(l_{k-2}^{\pm})^q$ when calculating $l_k^{\pm}$.

- To begin the induction we show that P_k is true when $k = 3$ and 4.
  - ∗ When $k = 3$ we have

$$(l_2)^{\frac{q+1}{2}} - w_2 = \left(s_0^{q+1} - s_1^2\right)^{\frac{q+1}{2}} - (s_1^{q+1} - s_2 s_0^q)$$

by definition and thus we see that $l_1^- = s_0$ divides $(l_2)^{\frac{q+1}{2}} - w_2$ as the terms not divisible by s_0^q, that is $(-s_1^2)^{\frac{q+1}{2}}$ and $-s_1^{q+1}$, cancel when $\frac{q+1}{2}$ is even.

Similarly we see that l_1^- does not divide

$$(l_2)^{\frac{q+1}{2}} + w_2 = \left(s_0^{q+1} - s_1^2\right)^{\frac{q+1}{2}} + (s_1^{q+1} - s_2 s_0^q)$$

but $l_1^+ = 1$ does.

Then define

$$\begin{aligned} l_3^+ &= \frac{(l_2)^{\frac{q+1}{2}} + w_2}{(l_1^+)^q} \\ &= \left(s_0^{q+1} - s_1^2\right)^{\frac{q+1}{2}} + s_1^{q+1} - s_2 s_0^q \qquad \text{and} \end{aligned}$$

$$\begin{aligned} l_3^- &= \frac{(l_2)^{\frac{q+1}{2}} - w_2}{(l_1^-)^q} \\ &= \frac{\left(s_0^{q+1} - s_1^2\right)^{\frac{q+1}{2}} - (s_1^{q+1} - s_2 s_0^q)}{s_0^q} \\ &= \frac{\left(s_0^{q+1} - s_1^2\right)^{\frac{q+1}{2}} - s_1^{q+1}}{s_0^q} + s_2. \end{aligned}$$

We note that both l_3^+ and l_3^- are irreducible and that the polynomials are not associates by considering the coefficients of the terms in s_2 in each.

Thus P_k is true in the case $k = 3$.

$*$ When $k = 4$ we see that, by definition, the coefficient of s_3 in the expressions $(l_3)^{\frac{q+1}{2}} \pm w_3$ is $\mp(l_2)^q$ and that of $(s_2)^{q+1}$ is equal to $((l_1)^{\frac{q+1}{2}} \pm w_1)^q$ by Lemma 5.10 and thus by definition to $(s_0{}^{\frac{q+1}{2}} \pm s_1)^q = (l_2^{\pm})^q$.

Now, any divisor of $(l_3)^{\frac{q+1}{2}} \pm w_3$ must divide the coefficient, $\mp(l_2)^q$ of s_3 and, as l_2 has no term in s_2, must also divide the coefficient $(l_2^{\pm})^q$ of $(s_2)^{q+1}$.

Now l_2^+ and l_2^- are irreducible and are not associates. Thus we see that the expression $(l_3)^{\frac{q+1}{2}} + w_3$ is not divisible by l_2^- and that the expression $(l_3)^{\frac{q+1}{2}} - w_3$ is not divisible by l_2^+.

Then as

$$l_4 = \frac{\left((l_3)^{\frac{q+1}{2}} + w_3\right)\left((l_3)^{\frac{q+1}{2}} - w_3\right)}{(l_2^+)^q (l_2^-)^q}$$

$(l_2^{\pm})^q$ must divide $(l_3)^{\frac{q+1}{2}} \pm w_3$. Thus we have the factors

$$\frac{(l_3)^{\frac{q+1}{2}} + w_3}{(l_2^+)^q} \quad \text{and} \quad \frac{(l_3)^{\frac{q+1}{2}} - w_3}{(l_2^-)^q} \qquad \text{of } l_4.$$

Now define

$$l_4^+ = \frac{(l_3)^{\frac{q+1}{2}} + w_3}{(l_2^+)^q} \quad \text{and} \quad l_4^- = \frac{(l_3)^{\frac{q+1}{2}} - w_3}{(l_2^-)^q}.$$

We note that, by definition, each polynomial $l_4^{\pm}$ is linear in s_3 and that the coefficient of s_3 in $l_4^{\pm}$ is $\frac{\mp(l_2)^q}{(l_2^{\pm})^q} = \mp(l_2^{\mp})^q$.

We now assume that l_4^+ is not irreducible and so let f^+ be an irreducible polynomial such that $f^+ | l_4^+$. Then as l_4^+ is linear in s_3 we have that $f^+ | -(l_2^-)^q$ and so as f^+ is assumed to be irreducible then $f^+ = l_2^-$. Similarly, assuming that l_4^- is not irreducible and letting f^- be an irreducible polynomial such that $f^- | l_4^-$ then $f^- = l_2^+$.

Then

$$l_2^{\mp} | l_4^{\pm} = \frac{(l_3)^{\frac{q+1}{2}} \pm w_3}{(l_2^{\pm})^q} \quad \text{and so} \quad l_2^{\mp} | (l_3)^{\frac{q+1}{2}} \pm w_3.$$

However, we have seen above that this is not the case and so can conclude that each of $l_4^{\pm}$ is irreducible.

Now

$$\begin{aligned} l_4^+ &= \frac{-(l_2)^q s_3 + (l_2^+)^q (s_2)^{q+1} + \dots}{(l_2^+)^q} = -(l_2^-)^q s_3 + (s_2)^{q+1} + \dots \quad \text{and} \\ l_4^- &= \frac{(l_2)^q s_3 + (l_2^-)^q (s_2)^{q+1} + \dots}{(l_2^-)^q} = -(l_2^+)^q s_3 + (s_2)^{q+1} + \dots \end{aligned}$$

so we see that l_4^+ and l_4^- are not associates.

Hence P_k is true in the case $k = 4$.

- Now assume the inductive hypothesis that P_k is true in the case $k = m$. That is l_m factorises as the product of the two irreducible polynomials l_m^+ and l_m^- that are not associates as defined below.

$$l_m^+ = \frac{(l_{m-1})^{\frac{q+1}{2}} + w_{m-1}}{(l_{m-2}^+)^q} \quad \text{and} \quad l_m^- = \frac{(l_{m-1})^{\frac{q+1}{2}} - w_{m-1}}{(l_{m-2}^-)^q}$$

Hence

$$(l_{m-1})^{\frac{q+1}{2}} \pm w_{m-1} = l_m^{\pm}(l_{m-2}^{\pm})^q$$

When $k = m + 2$ we have

$$l_{m+2} = \frac{\left[(l_{m+1})^{\frac{q+1}{2}} + w_{m+1}\right]\left[(l_{m+1})^{\frac{q+1}{2}} - w_{m+1}\right]}{(l_m^+)^q(l_m^-)^q}$$

and so consider the coefficients of s_{m+1} and $(s_m)^{q+1}$ in the expressions $(l_{m+1})^{\frac{q+1}{2}} \pm w_{m+1}$. The coefficient of s_{m+1} is $\mp(l_m)^q$ by definition and that of $(s_m)^{q+1}$ is $(l_{m-1}^{\frac{q+1}{2}} \pm w_{m-1})^q$ by Lemma 5.10 which by hypothesis is equal to $[l_m^{\pm}(l_{m-2}^{\pm})^q]^q$.

Thus we see that any divisor of $(l_{m+1})^{\frac{q+1}{2}} \pm w_{m+1}$ must divide $\mp l_m^q$ and as l_m has no term in s_m must also divide $[l_m^{\pm}(l_{m-2}^{\pm})^q]^q$. Thus we see that, as l_m^+ and l_m^- are irreducible and not associates by hypothesis, $(l_{m+1})^{\frac{q+1}{2}} \pm w_{m+1}$ is not divisible by $l_m^{\mp}$.

Then as l_{m+2} is a polynomial we see that $(l_m^{\pm})^q$ must divide $(l_{m+1})^{\frac{q+1}{2}} \pm w_{m+1}$. Thus we have the factors

$$\frac{(l_{m+1})^{\frac{q+1}{2}} + w_{m+1}}{(l_m^+)^q} \quad \text{and} \quad \frac{(l_{m+1})^{\frac{q+1}{2}} - w_{m+1}}{(l_m^-)^q} \quad \text{of } l_{m+2}$$

and so we can define

$$l_{m+2}^+ = \frac{(l_{m+1})^{\frac{q+1}{2}} + w_{m+1}}{(l_m^+)^q} \quad \text{and} \quad l_{m+2}^- = \frac{(l_{m+1})^{\frac{q+1}{2}} - w_{m+1}}{(l_m^-)^q}.$$

We note that, by definition, each polynomial $l_{m+2}^{\pm}$ is linear in s_{m+1} and that the coefficient of s_{m+1} in $l_{m+2}^{\pm}$ is $\frac{\mp(l_m)^q}{(l_m^{\pm})^q} = \mp(l_m^{\mp})^q$.

We now assume that l_{m+2}^+ is not irreducible and so let f^+ be an irreducible polynomial such that $f^+ | l_{m+2}^+$. Then as l_{m+2}^+ is linear in s_{m+1} we have that $f^+ | -(l_m^-)^q$ and so

as f^+ is assumed to be irreducible then $f^+ = l_m^-$. Similarly, assuming that l_{m+2}^- is not irreducible and letting f^- be an irreducible polynomial such that $f^-|l_{m+2}^-$ then $f^- = l_m^+$. Then

$$l_m^{\mp}|l_{m+2}^{\pm} = \frac{(l_{m+1})^{\frac{q+1}{2}} \pm w_{m+1}}{(l_m^{\pm})^q} \quad \text{and so} \quad l_m^{\mp}|(l_{m+1})^{\frac{q+1}{2}} \pm w_{m+1}.$$

However, we have seen above that this is not the case and so can conclude that each of $l_{m+2}^{\pm}$ is irreducible.

Now

$$\begin{aligned} l_{m+2}^+ &= \frac{-(l_m)^q s_{m+1} + (l_2^+)^q (s_m)^{q+1} + \dots}{(l_m^+)^q} = -(l_2^-)^q s_{m+1} + (s_m)^{q+1} + \dots \quad \text{and} \\ l_{m+2}^- &= \frac{(l_m)^q s_{m+1} + (l_m^-)^q (s_m)^{q+1} + \dots}{(l_m^-)^q} = -(l_m^+)^q s_{m+1} + (s_m)^{q+1} + \dots \end{aligned}$$

so we see that l_{m+2}^+ and l_{m+2}^- are not associates.

Thus P_k true in the case $k = m$ implies P_k true in the case $k = m + 2$. As P_k is true when $k = 3$ and $k = 4$ we deduce that P_k is true for all $k \geq 3$ when $q = 3 \mod 4$.

(ii) The proof for the case $q \equiv 1 \bmod 4$ proceeds as that in the case $q \equiv 3 \bmod 4$ but now $\frac{q+1}{2}$ is odd and from Lemma 5.10 the coefficient of $(s_{k-1})^{q+1}$ in $l_k^{\frac{q+1}{2}} \pm w_k$ is $-\left[(l_{k-2})^{\frac{q+1}{2}} \mp w_{k-2})\right]^q$.

□

5.3 Further analysis of the $l_k^{\pm}$ polynomials

Lemma 5.12. *Working in the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ the coefficient of s_{k-1} in l_k^+ for $k \geq 2$ is*

- $(-1)^k (l_{k-2}^-)^q$ *when* $q \equiv 3 \bmod 4$ *and*
- $(-1)^k (l_{k-2}^+)^q$ *when* $q \equiv 1 \bmod 4$.

and that in l_k^- for $k \geq 2$ is

- $(-1)^{k+1} (l_{k-2}^+)^q$ *when* $q \equiv 3 \bmod 4$ *and*
- $(-1)^{k+1} (l_{k-2}^-)^q$ *when* $q \equiv 1 \bmod 4$.

We can see that by definition the Lemma is true when $k = 2$ as $l_0^+ = l_0^- = 1$.

Initially the Lemma 5.12 was shown to be true in the case $q = 3$ for $k = 3, \ldots, 6$ and $q = 5$ for $k = 3, \ldots 5$ using CoCoA code as given in Appendix C Subsection C.2.2 with output given in Appendix C.3.

Proof. By definition the coefficient of s_{k-1} in $l_{k-1}^{\frac{q+1}{2}} + w_{k-1}$ is $(-1)^k (l_{k-2})^q)$ and that in $l_{k-1}^{\frac{q+1}{2}} - w_{k-1}$ is $(-1)^{k+1}(l_{k-2})^q)$ as seen in the proof of Theorem 5.11. The result then follows on dividing by l_{k-2}^+ or l_{k-2}^- as appropriate to the definitions of $l_k^\pm$ for $q \equiv 3 \bmod 4$ and $q \equiv 1 \bmod 4$ given in Theorem 5.11. □

5.4 The factorisation of the $l_k^{\pm}$ over the ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$

We have defined the l_k, l_k^+ and l_k^- in the ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ in §3.2 and in §5.1. We now define a map Q_n from the ring $A = \mathbb{F}_q[s_0, s_1, s_2, \ldots]$ to the ring $S = \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ determined by the choice of quadratic form

$$\xi_0 = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2$$

so that

$$\begin{aligned} Q_n : A &\longrightarrow S \\ s_j &\longmapsto \varepsilon x_1^{q^j+1} + \sum_{i=2}^{n} x_i^{q^j+1} \end{aligned}$$

Thus we see that the image of the polynomial l_n under this map is Λ_n and we define the images of l_k, l_k^+ and l_k^- as Λ_k, Λ_k^+ and Λ_k^- respectively. We note that the images Λ_k, Λ_k^+ and Λ_k^- are each invariants of the Orthogonal group $O(\xi_0)$ being polynomials in the ξ's.

The images of the l_k, l_k^+ and l_k^- are calculated explicitly under Q_n and we then consider how the polynomials Λ_n, Λ_{n+1}, $\Lambda_n^+, \Lambda_n^-, \Lambda_{n+1}^+$ and Λ_{n+1}^- factorise over the ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

5.4.1 Grouping of the monic vectors

The monic vectors, those on which the first non zero coefficient is 1, of the dual space V^*, with basis $x_1, x_2, \ldots x_n$, are separated into three sets. These sets are defined according to the value of the quadratic form s_0 on the corresponding vector in V under the map $\hat{Q}$ determined by the quadratic form ξ_0 as given in the statement of Lemma 1.23.

Definition 5.13. Given a vector space W of dimension n over $\mathbb{F}_q$ and basis $\mathcal{B} = \{x_1, x_2, \ldots, x_n\}$ of W we define a vector $w \in W$ to be *monic* with respect to the basis $\mathcal{B}$ if the first non zero component of w with respect to $\mathcal{B}$ is 1.

Lemma 5.14. *The number of monic vectors in the vector space W over $\mathbb{F}_q$ of dimension n is $\frac{q^n-1}{q-1}$ which is even when n is even and odd when n is odd.*

Proof. There are $q^n - 1$ non zero vectors W over $\mathbb{F}_q$. For each vector $w \in W$ there are $q-1$ vectors of the form kw for $k \in \mathbb{F}_q$ of which only one has its first non zero component equal to 1.

Thus there are $\frac{q^n-1}{q-1}$ monic vectors in W.

Now

$$\frac{q^n-1}{q-1} = \sum_{i=0}^{n-1} q^i.$$

As the number of summands is n and when q is odd each power of q is odd the total number of monic vectors is even when n is even and odd when n is odd. □

Definition 5.15. We define $\mathcal{V}$ to be the set of monic vectors in V^* and $\overline{\mathcal{V}}$ to be the product of these vectors that is

$$\overline{\mathcal{V}} = \prod_{x \in \mathcal{V}} x.$$

We now define the polynomials $\overline{\mathcal{Z}}$,$\overline{\mathcal{S}}$ and $\overline{\mathcal{N}}$ determined by the value of the quadratic form ξ_0 on the vectors in V as follows.

Definition 5.16. Let $\hat{Q}$ be the map from V to V^* determined by the quadratic form ξ_0 as defined in the statement of Lemma 1.23. Then define $\mathcal{Z}$ to be the set of vectors in V^* corresponding under the map $\hat{Q}$ to those in V on which the form ξ_0 is zero. That is

$$\mathcal{Z} = \{\hat{Q}(v) \in V^* | \xi_0(v) = 0\}.$$

Similarly define $\mathcal{S}$ to be the set of vectors in V^* corresponding under the map $\hat{Q}$ to those in V on which the form ξ_0 takes the value of a square in $\mathbb{F}_q^*$ and $\mathcal{N}$ to be the set of vectors in V^* corresponding to those in V on which the form takes the value of a non squares. That is

$$\mathcal{S} = \{\hat{Q}(v) \in V^* | \xi_0(v) = \sigma\} \quad \text{for } \sigma\text{a square in } \mathbb{F}_q^*$$

and

$$\mathcal{N} = \{\hat{Q}(v) \in V^* | \xi_0(v) = \nu\} \quad \text{for } \nu\text{a non square in } \mathbb{F}_q^*.$$

Then define

$$\overline{\mathcal{Z}} = \prod_{x \in \mathcal{Z}} x, \qquad \overline{\mathcal{S}} = \prod_{x \in \mathcal{S}} x \qquad \text{and} \qquad \overline{\mathcal{N}} = \prod_{x \in \mathcal{N}} x.$$

5.4.2 The factorisation of Λ_n over $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$

We wish to express Λ_n in terms of the the monic vectors and to that purpose recall that $\Lambda_n = \epsilon\ell^2$ from Equation 5.1 in Definition 5.1.

Lemma 5.17. *The polynomial ℓ is such that*

$$\ell^2 = \overline{\mathcal{V}}^2.$$

Proof. The coefficient of X in the polynomial

$$d_n(X) = \prod_{v \in V} (X - v)$$

is $(-1)^n c_{n,0}$ by Lemma 3.1 and the Dickson invariant $c_{n,0} = \ell^{q-1}$ by Lemma 3.4 so that the coefficient of X is $(-1)^n \ell^{q-1}$.

Now the vector space V over $\mathbb{F}_q$ is of dimension n so we can let $V = \{v_1, v_2, \ldots, v_{q^n}\}$ with $v_1 = 0$ without loss of generality. Then

$$d_n(X) = X \prod_{i=2}^{q^n} (X - v_i)$$

and so the coefficient of X in $d_n(X)$ is

$$(-1)^{q^n - 1} \prod_{i=2}^{q^n} v_i$$

which is

$$\prod_{i=2}^{q^n} v_i = \prod_{v \in V \setminus 0} v$$

as $q^n - 1$ is even when q is odd.

For each monic vector $\overline{v} \in \mathcal{V}$ there are $q - 1$ vectors $f\,\overline{v} \in V$ with $f \in \mathbb{F}_q^*$ and the product of these vectors is

$$\prod_{f \in \mathbb{F}_q^*} f\,\overline{v} = \overline{v}^{\,q-1} \prod_{f \in \mathbb{F}_q^*} f \; = - \, \overline{v}^{\,q-1} \qquad \text{by Lemma 2.8.}$$

The number of monic vectors is $|\mathcal{V}|$ which is odd or even as n is odd or even by Lemma 5.14. Thus the coefficient of X is

$$(-1)^{|\mathcal{V}|} \prod_{v \in \mathcal{V}} v^{q-1} = (-1)^n \prod_{v \in \mathcal{V}} v^{q-1} = (-1)^n \left(\prod_{v \in \mathcal{V}} v \right)^{q-1}.$$

Hence, as the coefficient is $(-1)^n \ell^{q-1}$ as discussed above,

$$(-1)^n \ell^{q-1} = (-1)^n \left(\prod_{v \in \mathcal{V}} v \right)^{q-1}.$$

Thus

$$\ell = \pm \prod_{v \in \mathcal{V}} v = \pm \overline{\mathcal{V}}$$

and so

$$\ell^2 = \overline{\mathcal{V}}^2$$

as required.

□

Corollary 5.18. *The polynomial*

$$\Lambda_n = \varepsilon \overline{\mathcal{V}}^2$$

5.4.3 The factorisation of $\Lambda_n^{\pm}$ and $\Lambda_{n+1}^{\pm}$ over $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$

CoCoA code has been used to factorise $\Lambda_n^{\pm}$ and $\Lambda_{n+1}^{\pm}$ over $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ where a quadratic form ξ_0 is specified for some small values of n and q. We take

$$\xi_0 = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2$$

so that the form is of plus type when $\varepsilon = 1$ that is $\xi_0 = Q_s$ or of minus type when $\varepsilon = \nu$ for some non square $\nu \in \mathbb{F}_q^*$ that is $\xi_0 = Q_n$ as defined in the statement of Lemma 2.18. An example of this code and output for some cases is given in Appendix D.

The CoCoA code is given Appendix D.1 where the values of n, q and ε are input. The code sets $n = 4$ and $q = 3$ and $\varepsilon = 1$. The output for this case is given in Appendix D.2.3. The code has also been implemented with $n = 4, q = 3$ and $\varepsilon = \nu$ and with $n = 4, q = 5$ with both $\varepsilon = 1$ and $\varepsilon = \nu$ with output also in Appendix D.2.3. Similar code has been implemented for the cases $n = 2$ and $q \leq 43$ for q prime for both $\varepsilon = 1$ and $\varepsilon = \nu$. Output for the cases prime $q \leq 17$ is given in Appendix D.2.1. For the cases $n = 3$ and prime $q \leq 13$, similar code is implemented with output given in Appendix D.2.2.

On the basis the output we make the following conjecture.

Conjecture 5.19. (i) Let

$$\xi_0 = Q_s = \sum_{i=1}^{n} x_i^2.$$

Then

$$\Lambda_n^+ = \kappa_1 \overline{\mathcal{Z}}\, \overline{\mathcal{N}}^2,$$

$$\Lambda_n^- = \kappa_2 \overline{\mathcal{Z}}\, \overline{\mathcal{S}}^2,$$

$$\Lambda_{n+1}^+ = \kappa_3 \overline{\mathcal{Z}}\, \overline{\mathcal{S}}^{q+1} \overline{\mathcal{N}}^{q+1}$$

and

$$\Lambda_{n+1}^- = 0$$

for some $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{F}_q^*$.

(ii) Let

$$\xi_0 = Q_s = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2$$

where ε is a non square in $\mathbb{F}_q^*$. Then

$$\Lambda_n^+ = \kappa_1 \overline{\mathcal{Z}}\, \overline{\mathcal{S}}^2,$$

$$\Lambda_n^- = \kappa_2 \overline{\mathcal{Z}}\, \overline{\mathcal{N}}^2,$$

$$\Lambda_{n+1}^+ = 0$$

and

$$\Lambda_{n+1}^- = \kappa_3 \overline{\mathcal{Z}}\, \overline{\mathcal{S}}^{q+1} \overline{\mathcal{N}}^{q+1}$$

for some $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{F}_q^*$.

We have shown Conjecture 5.19(i) to be true when

- $n = 2$ and prime $q \leq 43$ with $\kappa_1 = 2$, $\kappa_2 = \frac{1}{2}$ and $\kappa_3 = 2$,
- $n = 3$ and prime $q \leq 13$ with $\kappa_1 = 2$, $\kappa_2 = \frac{1}{2}$ and $\kappa_3 = 1$ when $q \equiv 3 \bmod 4$ and $\kappa_3 = 4$ when $q \equiv 1 \bmod 4$,
- $n = 4$ with $\kappa_1 = 1$, $\kappa_2 = 1$ and $\kappa_3 = 1$ when $q = 3$ and $\kappa_1 = -1$, $\kappa_2 = -1$when $q = 5$. In the case $n = 4, q = 5$ the expressions for $\Lambda_{n+1}^{\pm}$ have not been determined as the calculation is very large.

We have shown Conjecture 5.19(ii) to be true when

- $n = 2$ and prime $q \leq 43$ with $\kappa_1 = -\frac{1}{2}$, $\kappa_2 = -2\varepsilon$ and $\kappa_3 = -2$ when $q \equiv 3 \bmod 4$ and $\kappa_3 = -2\varepsilon$ when $q \equiv 1 \bmod 4$,
- $n = 3$ and prime $q \leq 13$ with $\kappa_1 = -\frac{\varepsilon}{2}$, $\kappa_2 = -2$ and $\kappa_3 = 1$ when $q \equiv 3 \bmod 4$ and $\kappa_1 = -\frac{1}{2}$, $\kappa_2 = -2\varepsilon$ and $\kappa_3 = 8 = 4\varepsilon$ when $q \equiv 1 \bmod 4$,
- $n = 4$ with $\kappa_1 = -1$, $\kappa_2 = 1$ and $\kappa_3 = -1$ when $q = 3$ and $\kappa_1 = -1$, $\kappa_2 = -2$when $q = 5$. In the case $n = 4, q = 5$ once again the expressions for $\Lambda^{\pm}_{n+1}$ have not been determined.

We note that the results are consistent with Corollary 5.18 as $\kappa_1\kappa_2 = \varepsilon$ in all the tested cases.

Chapter 6

Invariants of the orthogonal group generated from the Λ_k

In this chapter we generate further invariants of the Orthogonal group. The motivation for this derives from the need to calculate invariants more efficiently than in the calculation of the Chern Orbit classes of §3.3 or in the d_i invariants of Chapter 4.

In particular we generate invariants in the case $n = 4$, $q = 3$ and $\xi_0 = Q_s$ as defined in the statement of Lemma 2.18 so that in this case $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Thus we are concerned with invariants of the group $O^+(4, 3)$.

We present an algorithm to calculate invariants from the l_k polynomials introduced in Definition 5.2. The Algorithm is then implemented using CoCoA code for the case specified above, the code being given in Appendix E.1.

In the previous chapter we determined the irreducible factors, $l_k^{\pm}$, of the polynomial l_k in the ring $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ generated inductively following the algorithm detailed in Section 5.2. We use the polynomials l_k, l_k^+ and l_k^- together with their images under the Total Steenrod Operation $\mathcal{P}^\bullet$ of Definition 3.11 defined on the ring $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ to generate the new invariants. We have noted that the image of these expressions as polynomials in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$ are invariants of the Orthogonal group $O(\xi_0)$ for the particular choice of the non-singular quadratic form ξ_0 in $\mathbb{F}_q[x_1, x_2, \dots, x_n]$.

6.1 Preliminaries

Firstly we define the ring homomorphisms $Q^{\sigma}_{n,m}$ and $Q^{\nu}_{n,m}$ as follows.

Definition 6.1. Let A be the polynomial ring $\mathbb{F}_q[s_0, s_1, \ldots, s_n]$.

Then define the maps $Q^{\sigma}_{n,m}$ and $Q^{\nu}_{n,m}$ from the ring A to the ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ induced on $\mathbb{F}_q[s_0, s_1, \ldots, s_n]$ by mapping s_0 to a non-singular form ξ_0 in m variables, the forms being Q_s and Q_n respectively. These forms are given explicitly in the statement of Lemma 2.18.

Then the image of each s_k is defined to be ξ_k and thus is determined by the choice of ξ_0 through the application of the Steenrod algebra, the explicit formulas for the ξ_k having been given in Definition 5.2.

Thus we have

$$\begin{aligned} Q^{\sigma}_{n,m} : A &\longrightarrow \mathbb{F}_q[x_1, \ldots x_m] \\ s_k &\longmapsto \xi_k = \sum_{1}^{m} x_i^{q^k+1} \quad \text{k=0, 1, \ldots, n} \end{aligned}$$

and

$$\begin{aligned} Q^{\nu}_{n,m} : A &\longrightarrow \mathbb{F}_q[x_1, \ldots x_m] \\ s_k &\longmapsto \xi_k = \nu x_1^{q^k+1} + \sum_{2}^{m} x_i^{q^k+1} \quad \text{k=0, 1, \ldots, n} \end{aligned}$$

where ν is a non-square in $\mathbb{F}_q^*$.

We now consider the ring homomorphisms $Q^{\sigma}_{n,n}$ and $Q^{\nu}_{n,n}$ from A to $S = \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and in particular the kernel of these maps.

Observing that each of $\mathrm{Im}\,(Q^{\sigma}_{n,n})$ and $\mathrm{Im}\,(Q^{\nu}_{n,n})$ are spanned by $\xi_0, \xi_1, \ldots, \xi_n$ we present Lemma 6.6 concerning the algebraic independence of these polynomials. For this we have refered to [3] Chapter 5.

Firstly we introduce the Jacobian which can be use in determining the algebraic independence of a set of polynomials.

Definition 6.2. Given the vector function F with component functions $f_1, \ldots, f_m$ of the vector space V with basis $x_1, \ldots, x_n$ we define the *Jacobian matrix*, $\mathcal{J}_\mathcal{F}$, to be the matrix of first order partial derivatives of the f_i with respect to the x_i. That is the Jacobian

$$\mathcal{J}_F = \frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

The *Jacobian determinant* or *Jacobian*

$$|\mathcal{J}_\mathcal{F}| = \det\left(\frac{\partial f_i}{\partial x_i}\right)$$

is then the determinant of the Jacobian matrix.

Definition 6.3. A *perfect field* is one in which every finite extension is separable. That is the minimum polynomial of every element of the extension is separable).

Lemma 6.4 ([4]: Proposition 7.29)**.** *Every finite field is perfect.*

Lemma 6.5 (The Jacobian proposition)**.** [3] *Proposition 5.4.2*
Let $x_1, \ldots, x_n$ be algebraically independent indeterminates over a perfect field K. If $f_1, \ldots, f_n$ are elements of $K(x_1, \ldots, x_n)$ then $K(x_1, \ldots, x_n)$ is a finitely separable extension of $K(f_1, \ldots, f_n)$ if and only if the Jacobian determinant

$$\det\left(\frac{\partial f_i}{\partial x_i}\right) \neq 0.$$

Lemma 6.6. *Let ξ_0 be a non-singular quadratic form. Then let $\xi_k,\ k = 1, \ldots n$ be forms determined from ξ_0 by means of the Steenrod operations as presented in §3.2. Then $\xi_1, \xi_2 \ldots, \xi_n$ are algebraically independent.*

Proof. We have seen, by Lemma 2.18, that any non-singular quadratic form in n variables over a finite field is equivalent to the form

$$\varepsilon x_1^2 + \sum_{i=1}^{n} x_i^2$$

for some $\varepsilon \in \mathbb{F}_q^*$.

Then let F be the vector function with components $f_1, \ldots, f_n$ of the vector space $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ such that

$$f_k = \xi_k = \varepsilon x_1^{q^k+1} + \sum_{i=1}^{n} x_i^{q^k+1} \quad k = 1, \ldots, n$$

Thus we have

$$\frac{\partial f_k}{\partial x_1} = \varepsilon(q^k+1)x_1^{q^k} = \varepsilon x_1^{q^k}$$

and

$$\frac{\partial f_k}{\partial x_j} = x_j^{q^k} \quad j = 2, \ldots n.$$

Then the Jacobian, is equal to

$$|\mathcal{J}_{\mathcal{F}}| = \det\left(\frac{\partial f_i}{\partial x_i}\right) = \begin{vmatrix} \varepsilon x_1^q & x_2^q & \ldots & x_n^q \\ \varepsilon x_1^{q^2} & x_2^{q^2} & \ldots & x_n^{q^2} \\ \vdots & \ddots & \ddots & \vdots \\ \varepsilon x_1^{q^n} & x_2^{q^n} & \ldots & x_n^{q^n} \end{vmatrix}$$

which we observe is equal to $\varepsilon\ell^q$ where $\ell = \Delta_n(x_n)$ is defined in Lemma 3.4.

It follows that $|J_F|$ is non zero and so the functions $\xi_1, \xi_2, \ldots, \xi_n$ are algebraically independent by Lemma 6.5. □

Definition 6.7. Let R be a ring and P a prime ideal of R.

Then the *Krull dimension*, $\dim(R)$ of R is the maximum length of a chain of strict inclusions of prime ideals in R and ∞ if there are such chains of unbounded length.

The *height* of a prime ideal, P in the ring R is the length of a chain of strict inclusions of prime ideals contained in P.

Lemma 6.8 ([21]: Proposition 5.2.2)**.** *Let R be a polynomial ring over a field in n variables, that is $R = K[V]$ for some field K and n-dimensional vector space V. Then the Krull dimension of R is the dimension of V over the field K, that is* $\dim(R) = n$.

Lemma 6.9. *Let $Q^{\sigma}_{n,n}$ and $Q^{\nu}_{n,n}$ be the ring homomorphisms respectively of Definition 6.1.*

Then each of $\mathrm{Ker}\,(Q^{\sigma}_{n,n})$ *and* $\mathrm{Ker}\,(Q^{\nu}_{n,n})$ *is a prime ideal of height 1 in $A = \mathbb{F}_q[s_0, s_1, \ldots, s_n]$.*

Proof. We observe that the Krull dimension of the domain $A = \mathbb{F}_q[s_0, s_1, \ldots, s_n]$ of the map $Q^{\sigma}_{n,n}$ is $n+1$ as A is a polynomial ring on $n+1$ indeterminates and note that the Krull dimension of the polynomial ring $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is n.

Thus as $Im(Q^{\sigma}_{n,n}) \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ the Krull dimension of $Im(Q^{\sigma}_{n,n})$ is less than or equal to n.

We have seen in Lemma 6.6 that the images $\xi_1, \xi_1, \ldots \xi_n$ of $s_1, s_2, \ldots, s_n$ under this map are algebraically independent and so we note that the Krull dimension of $Im(Q^{\sigma}_{n,n})$ is n.

Now as, by the First Isomorphism theorem,

$$Im(Q^{\sigma}_{n,n}) \cong \mathbb{F}_q[s_0, s_1, \ldots, s_n]/Ker(Q^{\sigma}_{n,n})$$

we have that

$$\begin{aligned} \text{Krull dim}\,(Im(Q^{\sigma}_{n,n})) &= \text{Krull dim}\,(\mathbb{F}_q[s_0, s_1, \ldots, s_n]/Ker(Q^{\sigma}_{n,n})) \\ &= \text{Krull dim}\,(\mathbb{F}_q[s_0, s_1, \ldots, s_n]) - \text{ height } (/Ker(Q^{\sigma}_{n,n})). \end{aligned}$$

Thus we see that the kernel of the map has height 1. We note also that the kernel is a prime ideal of $\mathbb{F}_q[s_0, s_1, \ldots, s_n]$ as $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is an integral domain.

The argument for $\text{Ker}\,(Q^{\nu}_{n,n})$ is similar.

Thus we see that $\text{Ker}\,(Q^{\sigma}_{n,n})$ and similarly $\text{Ker}\,(Q^{\sigma}_{n,n})$ is a prime of height 1 in $\mathbb{F}_q[s_0, s_1, \ldots, s_n]$.

□

Conjecture 6.10. The kernel of the map $Q^{\sigma}_{k,k}$ is principal on l^{-}_{k+1} and that of the map $Q^{\nu}_{k,k}$ is principal on l^{+}_{k+1}.

We observe that every height 1 prime ideal is principal in a UFD and so $\text{Ker}\,(Q^{\sigma}_{n,n})$ and $\text{Ker}\,(Q^{\nu}_{n,n})$ are principal on some irreducible polynomial in R which being a polynomial ring is UFD.

We have seen that the polynomials l^{-}_{k+1} and l^{+}_{k+1} are irreducible in the ring $\mathbb{F}_q[s_0, s_1, \ldots, s_n]$. By calculation using CoCoA code we have seen that these polynomials are in the kernels of the maps $Q^{\sigma}_{k,k}$ and $Q^{\nu}_{k,k}$ respectively for $k = 2, \ldots, 5$ when $q = 3$. Thus in these cases we see that Conjecture 6.10 is true.

We now define the action of the Total Steenrod Operation on the ring $A = \mathbb{F}_q[s_0, s_1, s_2, \ldots]$.

Definition 6.11. Given a vector space V over $\mathbb{F}_q$ endowed with a quadratic form ξ_0 and polynomial rings $S = \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and $A = \mathbb{F}_q[s_0, s_1, s_2, \ldots]$ we can define a corresponding map

$$\begin{aligned} f = f_{V,\xi_0} : \quad &\longrightarrow \quad S \\ s_k \quad &\mapsto \quad \xi_k \end{aligned}$$

where the ξ_k for $k \geq 1$ are determined by ξ_0 as in Definition 3.5. The Total Steenrod Operation $\mathcal{P}^\bullet$ of Definition 3.11 acts on $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ as given in Lemma 3.12. Then define the action of $\mathcal{P}^\bullet$ on the ring A in such a way that

$$f(\mathcal{P}^\bullet(s_0)) = \mathcal{P}^\bullet(f(s_0))$$

for all possible maps f arising as above from a choice of (V, ξ_0) . Thus an induced action of the Steenrod Algebra is defined on the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ and we have

(i) $\mathcal{P}^\bullet(s_0) = s_0 - 2s_1 + s_0^q$,

(ii) $\mathcal{P}^\bullet(s_k) = s_k - s_{k-1}^q - s_{k+1} + s_k^q$, for all $k \geq 1$

From here onwards we concentrate in the main on the case $q \equiv 3(\bmod 4)$. The theory for the case $q \equiv 1(\bmod 4)$ is similar.

We present the following Lemma for the case $q \equiv 3(\bmod 4)$.

Lemma 6.12. *Working in the polynomial ring* $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$ *and with* $q \equiv 3(\bmod 4)$, *the polynomial*

$$l_k^+ \text{ is a factor of the expression } (l_{k-1}^\mp)^q \mathcal{P}^\bullet(l_k^+) \mp l_{k+1}^\pm \mathcal{P}^\bullet(l_{k-2}^-)^q$$

and the polynomial

$$l_k^- \text{ is a factor of } (l_{k-1}^\mp)^q \mathcal{P}^\bullet(l_k^-) \pm l_{k+1}^\pm \mathcal{P}^\bullet(l_{k-2}^+)^q$$

for $k = 2, \ldots, 5$ *when* $q = 3$.

This Lemma is seen to be true for $k = 2, \ldots, 5$ and $q = 3$ using the code in Appendix E.1.

Proof. We start by showing that the expressions $(l_{k-1}^\mp)^q \mathcal{P}^\bullet(l_k^+) \mp l_{k+1}^\pm \mathcal{P}^\bullet(l_{k-2}^-)^q$ are polynomials in the ring $\mathbb{F}_q[s_0, s_1, \ldots, s_{k-1}]$.

By definition and following Lemma 5.12 let

$$l_k^+ = \left((-1)^k l_{k-2}^-\right)^q \cdot s_{k-1} + f_k^+$$

where f_k^+ is a polynomial in $s_0, s_1, \ldots s_{k-2}$. Then

$$\begin{aligned}
\mathcal{P}^\bullet(l_k^+) &= \mathcal{P}^\bullet\left((-1)^k (l_{k-2}^-)^q \cdot s_{k-1} + f_k^+\right) \\
&= (-1)^k \left(\mathcal{P}^\bullet(l_{k-2}^-)\right)^q \cdot \mathcal{P}^\bullet(s_{k-1}) + \mathcal{P}^\bullet(f_k^+) \quad \text{as } \mathcal{P}^\bullet \text{ is a ring homomorphism} \\
&= (-1)^k \left(\mathcal{P}^\bullet(l_{k-2}^-)\right)^q (s_{k-1} - s_{k-2}^q - s_k + s_{k-1}^q) + \mathcal{P}^\bullet(f_k^+) \text{ by Definition 6.11.}
\end{aligned}$$

As f_k^+ is a polynomial in $s_0, s_1, \ldots s_{k-2}$ then $\mathcal{P}^\bullet(f_k^+)$ is a polynomial in $s_0, s_1, \ldots s_{k-1}$. Thus

$$\mathcal{P}^\bullet(l_k^+) = -(-1)^k \left(\mathcal{P}^\bullet(l_{k-2}^-)\right)^q \cdot s_k + \text{a polynomial in } s_0, s_1, \ldots s_{k-1}$$

so that the coefficient of s_k in $\mathcal{P}^\bullet(l_k^+)$ is $(-1)^{k+1}\left(\mathcal{P}^\bullet(l_{k-2}^-)\right)^q$.

By Lemma 5.12 the coefficient of s_k in l_{k+1}^+ is $(-1)^{k+1}(l_{k-1}^-)^q$. We note that each of the polynomials l_{k-1}^q and $\mathcal{P}^\bullet(l_{k-2}^q$ contain no term in s_k.

Thus we see that the terms in s_k in the expression $(l_{k-1}^-)^q\mathcal{P}^\bullet(l_k^+) - l_{k+1}^+\mathcal{P}^\bullet(l_{k-2}^-)^q$ cancel and so the expression is a polynomial in the ring $\mathbb{F}_q[s_0, s_1, \ldots s_{k-1}]$ as required.

Similarly, as the coefficient of s_k in l_{k+1}^- is $(-1)^{k+2}(l_{k-1}^+)^q$, the terms in s_k in the expressions $(l_{k-1}^+)^q\mathcal{P}^\bullet(l_k^+) + l_{k+1}^-\mathcal{P}^\bullet(l_{k-2}^-)^q$ cancel so the expression is a polynomial in the ring $\mathbb{F}_q[s_0, s_1, \ldots s_{k-1}]$.

We now consider the map $Q_{k-1,k-1}^\nu$ of Definition 6.1, from $\mathbb{F}_q[s_0, s_1, \ldots, s_{k-1}]$ to the vector space V of dimension $k-1$. We have proposed in Conjecture 5.19 that l_k^+ and $l_{k+1}^\pm$ are in the kernel of $Q_{k-1,k-1}^\nu$ and this has been shown to be true for $k = 2, \ldots, 5$ when $q = 3$ by calculation as presented following the conjecture.

Hence in these cases the kernel also contains $\mathcal{P}^\bullet(l_k^+)$ and thus the expression $(l_{k-1}^\mp)^q\mathcal{P}^\bullet(l_k^+) \mp l_{k+1}^\pm\mathcal{P}^\bullet(l_{k-2}^-)^q$.

We proposed in Conjecture 6.10 that the Kernel of the map $Q_{k-1,k-1}^\nu$ is the prime ideal generated by l_k^+ and for $k = 2, \ldots, 5$ and $q = 3$ this is seen to be the case by calculation as detailed following the conjecture.

Thus, in these cases, we see that $(l_{k-1}^\mp)^q\mathcal{P}^\bullet(l_k^+) \mp l_{k+1}^\pm\mathcal{P}^\bullet(l_{k-2}^-)^q$ is a multiple of l_k^+ as required.

Similarly we consider the expressions $(l_{k-1}^\mp)^q\mathcal{P}^\bullet(l_k^-) \pm l_{K+1}^\pm\mathcal{P}^\bullet(l_{k-2}^+)^q$ and can see that the terms in s_k in these expressions cancel so that these too are in the ring $\mathbb{F}_q[s_0, s_1, \ldots, s_{k-1}]$.

Again we have that l_k^- and $l_{k+1}^{\pm}$ and thus $\mathcal{P}^\bullet(l_k^-)$ and so $(l_{k-1}^{\mp})^q\mathcal{P}^\bullet(l_k^-) \pm l_{K+1}^{\pm}\mathcal{P}^\bullet(l_{k-2}^+)^q$ are in the kernel of the map $Q^q_{k-1,k-1}$. The kernel is seen to be principal on l_k^- for $k = 2, \ldots, 5$ and $q = 3$ and thus we see that in these cases the expressions are multiples of l_k^- as required. □

Conjecture 6.13. Working in the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \ldots]$

$$\mathcal{P}^\bullet(l_k^-) \text{ is a factor of the expressions } (l_{k-1}^{\mp})^q\mathcal{P}^\bullet(l_k^+) \mp l_{k+1}^{\pm}\mathcal{P}^\bullet(l_{k-2}^-)^q$$

and

$$\mathcal{P}^\bullet(l_k^-) \text{ is a factor of } (l_{k-1}^{\mp})^q\mathcal{P}^\bullet(l_k^-) \pm l_{K+1}^{\pm}\mathcal{P}^\bullet(l_{k-2}^+)^q.$$

We have seen this to be true using CoCoA code given in Appendix E in the case $k = 2, \ldots 5$ and $q = 3$.

6.2 The adjusted matrices

We define the matrices

$$\mathcal{S}_n(X) = D_n(X)\, B\, \hat{D}_n \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$$

where $D_n(X)$ is the Dickson matrix defined in the proof of Lemma 3.1, the matrix B is introduced at the start of §5.1 for the definition of the l_n polynomial and

$$\hat{D}_n = \begin{pmatrix} x_1 & x_1^q & x_1^{q^2} & \ldots & x_1^{q^{n-1}} & 0 \\ x_2 & x_2^q & x_2^{q^2} & \ldots & x_2^{q^{n-1}} & 0 \\ x_3 & x_3^2 & x_3^{q^2} & \ldots & x_3^{q^{n-1}} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_n & x_n^q & x_n^{q^2} & \ldots & x_n^{q^{n-1}} & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Note that the matrix $\hat{D}_n$ is derived from the matrix $D_{n-1}(x_n)$.

Hence we have

$$\mathcal{S}_n(X) = \begin{pmatrix} \xi_0 & \xi_1 & \xi_2 & \xi_3 & \dots & \xi_{n-1} & X \\ \xi_1 & \xi_0^q & \xi_1^q & \xi_2^q & \dots & \xi_{n-2}^q & X^q \\ \xi_2 & \xi_1^q & \xi_0^{q^2} & \xi_1^{q^2} & \dots & \xi_{n-3}^{q^2} & X^{q^2} \\ \xi_3 & \xi_2^q & \xi_1^{q^2} & \xi_0^{q^3} & \dots & \xi_{n-4}^{q^3} & X^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \\ \xi_{n-1} & \xi_{n-2}^q & \xi_{n-3}^{q^2} & \xi_{n-4}^{q^3} & \dots & \xi_0^{q^{n-1}} & X^{q^{n-1}} \\ \xi_n & \xi_{n-1}^q & \xi_{n-2}^{q^2} & \xi_{n-3}^{q^3} & \dots & \xi_1^{q^{n-1}} & X^{q^n} \end{pmatrix} \tag{6.1}$$

We now define the matrix $S_k(X)$ in the polynomial ring $\mathbb{F}_q[s_0, s_1, s_2, \dots]$ so that for $k = n$ the matrix $\mathcal{S}_n(X)$ is the image of $S_n(X)$ under one of the maps $Q^{\sigma}_{k,k}$ or $Q^{\nu}_{k,k}$ from $\mathbb{F}_q[s_0, s_1, \dots, s_n]$ to $\mathbb{F}_q[x_1, x_2, \dots, x_n]$ depending on the choice of image ξ_0 of s_0.

$$S_k(X) = \begin{pmatrix} s_0 & s_1 & s_2 & s_3 & \dots & s_{k-1} & X \\ s_1 & s_0^q & s_1^q & s_2^q & \dots & s_{k-2}^q & X^q \\ s_2 & s_1^q & s_0^{q^2} & s_1^{q^2} & \dots & s_{k-3}^{q^2} & X^{q^2} \\ s_3 & s_2^q & s_1^{q^2} & s_0^{q^3} & \dots & s_{k-4}^{q^3} & X^{q^3} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \\ s_{k-1} & s_{k-2}^q & s_{k-3}^{q^2} & s_{k-4}^{q^3} & \dots & s_0^{q^{k-1}} & X^{q^{k-1}} \\ s_k & s_{k-1}^q & s_{k-2}^{q^2} & s_{k-3}^{q^3} & \dots & s_1^{q^{k-1}} & X^{q^k} \end{pmatrix} \tag{6.2}$$

We define the matrices $M_k^+(X)$ and $M_k^+(X)$ adjusted from the matrix $S_k(X)$ by removing the ξ_k term. We consider the case for $q \equiv 3 \bmod 4$ when the matrix $M_k^+(X)$ is found by multiplying the first column of the matrix $S_k(X)$, and thus the determinate of the matrix, by $(l_{k-1}^-)^q$ and then adding the term $(-1)^k l_{k+1}^+$ to the last entry in the first column.

We have shown that in this case the coefficient of s_k in the expression l_{k+1}^+ is $(-1)^{k+1}(l_{k-1}^-)^q$ in Lemma 5.12 so in $(-1)^{k+1} l_{k+1}^+$ we have term $-(l_{k-1}^-)^q$. Thus the s_k term of this entry of the matrix cancels and so the only entry containing s_k in the matrix is removed. Thus the determinant of the matrix $M_k^+(X)$ is in the ring $\mathbb{F}_q[s_0, s_1, \dots, s_{k-1}][X]$.

We note that if l_{k+1}^+ is in the kernel of the map $Q^{\sigma}_{k,k}$ adding the term to an entry of the matrix has no effect on the image of the determinant under this map and as we have seen this is the case when $k = 2, \dots, 5$ and $q = 5$.

The matrix $M_k^-(X)$ is adjusted in a similar way from the matrix $S_k(X)$ with, in the case for $q \equiv 3 \bmod 4$, the first column being multiplied by $(l_{k-1}^+)^q$ and the term $(-1)^{k+1} l_{k+1}^-$ being added to the last entry in this column so that the term is s_k is removed. The coefficient of s_k in l_{k+1}^+ is $(-1)^{k+2}(l_{k-1}^-)^q$ when $q \equiv 3 \bmod 4$.

We note that the expression $(-1)^k l_{k+1}^-$ is in the kernel of the map $Q_{k,k}^\nu$ for $k = 2, \ldots, 5$ so that again adding this term to an entry of the matrix has no effect on the image of the determinant under this map.

Conjecture 6.14. Given the matrices $M_n^\pm(X)$ defined above then the determinant of $M_n^+(X)$ is divisible by the product $l_k \cdot \mathcal{P}^\bullet(l_{k-1}^-)$ and the determinant of $M_n^-(X)$ is divisible by the product $l_k \cdot \mathcal{P}^\bullet(l_{k-1}^+)$.

We have shown this conjecture to be true in the cases $k = 2, \ldots, 5$ for $q = 3$ using CoCoA code given in Appendix E.1.

6.3 An algorithm to determine new invariants of the Orthogonal groups $O^+(4,3)$ and $O^-(4,3)$ from the l_k invariants

In this section we outline an algorithm to generate the new invariants a_3 and a_2 of the Orthogonal groups $O(Q_s) \cong O^+(4,3)$ and $O(Q_n) \cong O^-(4,3)$ where the non-singular quadratic forms Q_s and Q_n are defined explicitly in the statement of Lemma 2.18.

The algorithm is implemented with the CoCoA code given in Appendix E.1. The output from the code is given in Appendix E.2.

We give the explicit expressions for the invariants a_2 and a_3 for the Orthogonal group $O(Q_s)$ in Appendix E.3.

The algorithm is as follows.

- The rings $S = \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and $A = \mathbb{F}_q[s_0, s_1, \ldots, s_n]$ are defined and variables n and q set up. The polynomials $l_k^\pm$ are generated for $k = 0, \ldots 5$ in the ring A.
- The images of each of the $l_k^\pm$ for $k = 0, \ldots, 5$ are calculated under the Total Steenrod operation $\mathcal{P}^\bullet$ as given in Definition 6.11.
- The maps $Q_{k,k}^\sigma$ and $Q_{k,k}^\nu$ are defined from A to S as given in Definition 6.1.

- The expressions given in Lemma 6.12 are calculated as $b_k^{\pm}$ and $c_k^{\pm}$ and the resulting polynomials divided by the expressions for $l_k^{\pm}$ and $\mathcal{P}^{\bullet}((l_{k-1})^q)$ as appropriate to Lemma 6.12 and Conjecture 6.13. The resulting expressions are tested for type thus checking the conjectured divisibility.

- The matrix $S_k(X)$ is defined as in Equation 6.2 and the matrix $S_k(1)$ used to define and the matrices M_k^+ and M_k^- being the matrices $M_k^+(X)$ and $M_k^-(X)$ as given in the discussion following Equation 6.2 with $X = 1$.

- The expressions d_k^+ and d_k^- are defined as

$$d_k^+ = \frac{\mathrm{Det}\,(M_k^+)}{l_k \cdot \mathcal{P}^{\bullet}(l_{k-1}^-)}$$

and

$$d_k^- = \frac{\mathrm{Det}\,(M_k^-)}{l_k \cdot \mathcal{P}^{\bullet}(l_{k-1}^+)}.$$

The type of these expressions is found to test the proposed divisibility of Conjecture 6.14.

- A dummy variable is now introduced. The Total Steenrod algebra is now defined with dummy variable included.

The images of the $l_k^{\pm}$ under this operation are calculated.

- The Matrices $S_k(X), M_k^+(X)$ and $M_k^-(X)$ are defined.

- The Chern orbit polynomials are defined. The newly generated invariants are compared with the Chern Orbit classes.

- For a given type of non-singular quadratic form the calculation of the new invariants then proceeds as follows. We give the procedure for plus type quadratic form.

  - The expressions d_k^+, b_k^+ and c_k^+ are calculated as presented above but including the dummy variable. We check to see that in fact

$$(d_k^+)^2 = b_k^+ c_k^+$$

  - The expression d_k^+/b_k^+ is calculated as a rational expression. The numerator and denominator of the resultant expression being the d_k^+ and b_k^+ with common factors removed. These polynomials now become our concern.

We note that each of these expressions being polynomials in the ξ_j's is an invariant of the Orthogonal group $O(\xi_0)$.

- We consider the numerator of the reduced rational function as a polynomial in the dummy variable and are in particular are concerned with the coefficients of degree 18 and 24; these values being the degrees of the Dickson invariants c_3 and c_2 each divided by $q = 3$. The denominator of d_k^+/b_k^+ can be used in the same way to give further invariants.
- We find the images of these coefficients under the map $Q_{k,k}^{\sigma}$ and on discovering that the image polynomials are divisible by the chosen quadratic form ξ_0 we divide the resulting polynomials by ξ_0 to give the new invariants which we denote a_3 and a_2.
- We test to see whether expressions a_3 and a_2 are in fact Chern Orbit classes.

Implementing the algorithm we can calculate the polynomials a_3 and a_2 for both plus type and minus type quadratic forms. We give the explicit expressions for a_3 and a_2 for the case $\xi_0 = Q_s$ in Appendix E.3 these being invariants of the Orthogonal group $O^+(4,3)$.

In this case we see that a_3 is equal to the Chern Orbit Class coefficients of the Chern polynomial $\chi_{\mathcal{O}_2^*}(X)$ as defined in §3.3.

Chapter 7

The ring of invariants of the orthogonal group

In this chapter we give an explicit presentation of the ring of invariants of the Orthogonal group $O^+(4,3)$ as $O(\xi_0)$ where the quadratic form defining the group is $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$. We do this in order to give an example of how the ideas presented in this thesis might be used to give an explicit presentation of the ring of invariants of the orthogonal group in the general case in odd characteristic. We note that in [8] the ring of invariants of the Orthogonal group $O^+(4,q)$ is presented with explicit generators.

In the first section we present a ring generated by some invariants of $O(x_1^2 + x_2^2 + x_3^2 + x_4^2)$ and we propose that this ring contains all the invariants of the Orthogonal group. At the end of §7.1 we calculate a relation on this ring and thus are able to give a presentation which we prove to be the ring of invariants $\mathbb{F}_3[x_1, x_2, x_3, x_4]^{O(\xi_0)}$ in §7.2.

7.1 The ring $\mathbb{F}_3\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle$

We restrict our attention to $O(\xi_0)$ where $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$, a non-singular quadratic form in $\mathbb{F}_3[x_1, x_2, x_3, x_4]$.

In this case we have established, in previous chapters, the existence of invariants of $O(\xi_0)$ of degree 18 and of degree 24. In Definition 3.23 we presented the invariants h_3 and h_2, determined as Chern orbit classes. Then in Definition 4.5 we presented the invariants d_3 and d_2 determined

from the Dickson invariants.

Being motivated to discover the differences between these pairs of invariants we investigate whether the differences can be written as polynomials in the invariants ξ_k as given in Definition 3.5. We discover, using CoCoA code, that the difference $d_3 - h_3$ can be expressed in terms of ξ_0, ξ_1 and ξ_2. Thus we give h_3 explicitly in terms of d_3, ξ_0, ξ_1 and ξ_1 below:

$$h_3 = d_3 - \xi_0^2\xi_1(\xi_0\xi_1^2 - \xi_2). \tag{7.1}$$

Similarly, by calculation, we find that the difference $d_2 - h_2$ can be expressed in terms of ξ_0, ξ_1, ξ_2 and the invariant d_3 and thus h_2 is given explicitly in terms of d_2, d_3, ξ_0, ξ_1 and ξ_1 below:

$$h_2 = d_2 - d_3\xi_0\xi_1 + \xi_0^{12} + \xi_0^4\xi_1^4 + \xi_1^6 + \xi_0^2\xi_2^2 - \xi_0^7\xi_1. \tag{7.2}$$

In Chapter 6 we generated further invariants, in particular for the case $n = 4$ and $q = 3$ we generated the invariants a_3, a_2 of $O(x_1^2 + x_2^2 + x_3^2 + x_4^2)$. The explicit expressions for a_3 and a_2 are given in Appendix E.3. By calculation using CoCoA code we see that these too can be expressed in terms of d_2, d_3, ξ_0, ξ_1 and ξ_1 as below.

$$a_3 = -\xi_0^7\xi_1 - \xi_0^5\xi_1^2 + \xi_0^2\xi_1\xi_2 - \xi_1^2\xi_2 - d_3 \tag{7.3}$$

$$a_2 = \xi_0^{12} - \xi_0^8\xi_1^2 - \xi_0^6\xi_1^3 + \xi_0^4\xi_1^4 - \xi_0^2\xi_1^5 + \xi_1^6 + (\xi_0^5\xi_1 - \xi_0^7)\xi_2 + (\xi_0^3\xi_1^2 + \xi_0\xi_1^3 - \xi_0^2 - \xi_1)\xi_2^2 + (\xi_0^3 + \xi_0\xi_1)d_3 - d_2 \tag{7.4}$$

Noting the expressions for h_2, h_3, a_2, and a_3 given in Equations 7.1, 7.2, 7.3 and 7.4 we observe that each of these invariants is in the sub ring $\mathbb{F}_3\langle\xi_0, \xi_1, \xi_2, d_3, d_2\rangle$ of $\mathbb{F}_3[x_1, x_2, x_3, x_4]$.

Thus we are motivated to propose that the sub ring

$$R_0 = \mathbb{F}_3\langle\xi_0, \xi_1, \xi_2, d_3, d_2\rangle \tag{7.5}$$

of $S = \mathbb{F}_3[x_1, x_2, x_3, x_4]$ contains all the invariants of $\mathbb{F}_3[x_1, x_2, x_3, x_4]^{O(\xi_0)}$ where each of ξ_0, ξ_1, ξ_2, d_3 and d_2 are taken to be the polynomials in the indeterminates x_1, x_2, x_3, x_4 previously defined. That is $\xi_k = \sum_{i=1}^4 x_i^{3^k+1}$ and the explicit expressions for d_3 and d_2 as polynomials in $x_1, \ldots, x_4$ are given in Appendix B.5. Further to this we propose that $R_0 = \mathbb{F}_3\langle\xi_0, \xi_1, \xi_2, d_3, d_2\rangle$ is the ring of invariants of $O(\xi_0)$.

We note that the ring R_0 has five generators and as R_0 is a sub ring of S of four indeterminates and we look for a relation on R_0. To this end we consider the ring homomorphism defined below from the polynomial ring

$$A_0 = \mathbb{F}_3[s_0, s_1, s_2, t_3, t_2] \tag{7.6}$$

to the ring R_0 determined by the expressions for each of the polynomials ξ_0, ξ_1, ξ_2, d_3 and d_2 previously defined.

Definition 7.1. Let A_0 be the polynomial ring $\mathbb{F}_3[s_0, s_1, s_2, t_3, t_2]$ and let $R_0 = \mathbb{F}_3\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle$ be the subring of S as given in Equation 7.5.

Then define the ring homomorphism Q_4^+ as follows.

$$\begin{aligned} Q_4^+ : A_0 &\longrightarrow R_0 \subseteq S \\ s_k &\longmapsto \xi_k = \sum_{i=1}^{4} x_i^{3^k+1} \qquad \text{for } k = 0, \ldots, 2 \\ t_j &\longmapsto d_j(x_1, x_2, x_3, x_4) \qquad \text{for } j = 2, 3 \end{aligned}$$

where the functions $d_j(x_1, x_2, x_3, x_4)$ are given explicitly in Appendix B.5.

Lemma 7.2. *The ring homorphism Q_4^+ presented in Definition 7.1 has kernel generated by the polynomial*

$$\rho = -s_0^{11}s_1^2 - s_0^7 s_1^4 + s_0^{10}s_2 + s_0^3 s_1^6 - s_0^6 s_1^2 s_2 - s_0^2 s_1^4 s_2 + s_0 s_1^2 s_2^2 + s_2^3 - t_2(s_0^3) + t_3(s_1 s_0^4 + s_1^3)$$

Proof. The generators of the kernel of Q_4^+ have been calculated using the CoCoa code given in Appendix F.3 together with the output. The result being that the kernel is generated by the single polynomial ρ. □

Thus we have the relation ρ on the ring A_0 and so define the ring

$$T = A_0/(\rho) \tag{7.7}$$

where A_0 is the polynomial ring $\mathbb{F}_3[s_0, s_1, s_2, t_3, t_2]$ and ρ the relation given in Lemma 7.2.

Lemma 7.3. *The ring $T = A_0/(\rho)$ of Equation 7.7 is isomorphic to R_0.*

Proof. Given the ring homomorphism Q_4^+ of Equation 7.1 we have $\mathrm{Ker}\,(Q_4^+) = (\rho)$ and $\mathrm{Im}\,(Q_4^+) = R_0$. Thus by the First Isomorphism Theorem $T = A_0/(\rho) \cong R_0$. □

We now propose that the ring of invariants $\mathbb{F}_3[x_1, x_2, x_3, x_4]^{O(\xi_0)}$ is the ring $R_0 = T/(\rho)$.

Firstly we prove the following Lemma regarding the ring R_0 showing that the ring of Dickson Invariants is contained in R_0.

Lemma 7.4. *Let R_c be the ring $\mathbb{F}_q[c_3, c_2, c_1, c_0]$ where c_i, $i = 0, \ldots, 3$ are the Dickson invariants of $GL(4, 3)$.*

Then $R_c \subseteq R_0$ where R_0 is the ring defined in Equation 7.5.

Proof. In Chapter 4 we established the polynomials ϕ_i in the ξ_k and the polynomials d_i presented implicitly in Definition 4.5.

Thus we have

$$\begin{aligned} c_3 &= d_3^q - (\xi_0\xi_1^{13} - \xi_0^4\xi_1^9\xi_2 - \xi_0^{10}\xi_1\xi_2^3 + \xi_0^{13}\xi_3 + \xi_1^{11}\xi_2 - \xi_0^9\xi_1^2\xi_3 + \xi_0\xi_1^3\xi_2^4 - \xi_0\xi_1^6\xi_3 \\ &\quad + \xi_1\xi_2^5 - \xi_1^4\xi_2\xi_3 - \xi_0^3\xi_2^2\xi_3) \\ &= d_3^q - (\xi_0\xi_1^{13} - \xi_0^4\xi_1^9\xi_2 - \xi_0^{10}\xi_1\xi_2^3 + \xi_1^{11}\xi_2 + \xi_0\xi_1^3\xi_2^4 + \xi_1\xi_2^5) \\ &\quad - \xi_3(\xi_0^{13} - \xi_0^9\xi_1^2 - \xi_0\xi_1^6 - \xi_1^4\xi_2 - \xi_0^3\xi_2^2) \end{aligned}$$

$$\begin{aligned} c_2 &= d_2^q - (\xi_0^{31}\xi_2 - \xi_0^2 8\xi_1^4 - \xi_0^{27}\xi_1^2\xi_2 + \xi_0\xi_1^{10}\xi_2^3 - \xi_0^4\xi_1^9\xi_3 + \xi_1^{11}\xi_3 - \xi_0\xi_2^7 + \xi_0\xi_1^3\xi_2^3\xi_3 \\ &\quad - \xi_1\xi_2^4\xi_3 + \xi_1^4\xi_3^2 - \xi_0^3\xi_2\xi_3^2) \\ &= d_2^q - (\xi_0^{31}\xi_2 - \xi_0^2 8\xi_1^4 - \xi_0^{27}\xi_1^2\xi_2 + \xi_0\xi_1^{10}\xi_2^3 - \xi_0\xi_2^7 + \xi_0\xi_1^3\xi_2^3\xi_3 \\ &\quad - \xi_3(\xi_1^{11} - \xi_1\xi_2^4 - \xi_0^4\xi_1^9) \\ &\quad - \xi_3^2(\xi_1^4 - \xi_0^3\xi_2) \end{aligned}$$

$$\begin{aligned} c_1 &= d_1^q - (\xi_0^{37}\xi_1 - \xi_0^{28}\xi_1^3\xi_2 - \xi_0^{27}\xi_1\xi_2^2 - \xi_0\xi_1^{19} + \xi_0\xi_1^9\xi_2^4 + \xi_0\xi_1^{12}\xi_3 - \xi_0^{10}\xi_2^3\xi_3 - \xi_1^{10}\xi_2\xi_3 \\ &\quad - \xi_0^9\xi_1\xi_3^2 + \xi_2^5\xi_3 + \xi_1^3\xi_2\xi_3^2) \\ &= d_1^q - (\xi_0^{37}\xi_1 - \xi_0^{28}\xi_1^3\xi_2 - \xi_0^{27}\xi_1\xi_2^2 - \xi_0\xi_1^{19} + \xi_0\xi_1^9\xi_2^4 \\ &\quad - \xi_3(\xi_0\xi_1^{12} - \xi_0^{10}\xi_2^3 - \xi_1^{10}\xi_2 + \xi_2^5) \\ &\quad - \xi_3^2(\xi_1^3\xi_2 - \xi_0^9\xi_1) \end{aligned}$$

By calculation using the CoCoA code given in Appendix F.1 we have shown ξ_3 to be in the ring R_0 as:

$$\xi_3 = d_3(\xi_0^5 - \xi_0\xi_1^2 - \xi_2) - d_2(\xi_1) - \xi_0^8\xi_1^3 + \xi_0^4\xi_1^5 - \xi_0^7\xi_1\xi_2 - \xi_1^7 - \xi_0^3\xi_1^3 + \xi_0^2\xi_1\xi_2^2\xi_2 \tag{7.8}$$

We can then substitute for ξ_3 using Equation 7.8 in the equations for c_3 and c_2 above and so have these as polynomials in ξ_0, ξ_1, ξ_2, d_3 and d_2 and thus see that

$$c_3, c_2 \in R_0$$

as required.

Again by calculation using the CoCoA code given in Appendix F.1 with the polynomial input as d_1 in place of ξ_3 we have shown d_1 to be in R_0 as below. The explicit expression for d_i as a polynomial in the x_i is given in Appendix B.5.

$$d_1 = d_3(\xi_1^2 - \xi_0^4) + \xi_0^1 1\xi_1 + \xi_0^7\xi_1^3 - \xi_0^3\xi_1^5 + \xi_0^6\xi_1\xi_2 + \xi_0^2\xi_1^3\xi_2 - \xi_0\xi_1\xi_2^2 \tag{7.9}$$

We can then substitute for d_1 and ξ_3 using Equations 7.8 and 7.9 in the equation for c_1 above so that we have c_1 as a polynomial in ξ_0, ξ_1, ξ_2, d_3 and d_2 and thus see that

$$c_1 \in R_0$$

as required.

We recall that if

$$\xi_0 = \varepsilon x_1^2 + \sum_{i=2}^{n} x_i^2$$

then $\Lambda_n = \epsilon\ell^2$ from Equation 5.1 in Definition 5.1 where the polynomial $\ell = \Delta_{n-1}(x_n)$ is given in the statement of Lemma 3.4.

We have that $c_0 = \ell^{q-1}$ from Lemma 3.4 and so in the case for $q = 3$ we have $\Lambda_n = \varepsilon c_0$.

When $\xi_0 = x_1^2 + x_2^2 + x^3 + x_4^2$ the value of ε is 1 and so

$$c_0 = \Lambda_4 = \begin{vmatrix} \xi_0 & \xi_1 & \xi_2 & \xi_3 \\ \xi_1 & \xi_0^3 & \xi_1^3 & \xi_2^3 \\ \xi_2 & \xi_1^3 & \xi_0^9 & \xi_1^9 \\ \xi_3 & \xi_2^3 & \xi_1^9 & \xi_0^{27} \end{vmatrix}$$

by Definition 5.1. We can substitute for ξ_3 again using Equation 7.8 and so have c_0 as a polynomial in ξ_0, ξ_1, ξ_2, d_3 and d_2 and thus see that

$$c_0 \in R_0$$

as required.

Thus we have $c_i \in R_0$ for $i = 0, 1, 2, 3$ and so $R_c \subseteq R_0$. □

7.2 The Ring of invariants $O^+(4, 3)$

Letting S be the polynomial ring $\mathbb{F}_3[x_1, x_2, x_3, x_4]$ we wish to prove that the ring

$$R_0 = \mathbb{F}_q\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle \subseteq S$$

as given in Definition 7.5 is the ring of invariants $S^{O(\xi_0)}$ when $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

We show first that the field of fractions of the ring R_0 is equal to the field of fractions of $S^{O(\xi_0)}$, the fixed field of $O(\xi_0)$, by application of the Fundamental Theorem of Galois Theory. A summary of Galois theory is given in [4] Section 8.2. We give a brief presentation of the theorem below.

Definition 7.5. Let K/F be a field extension. Then K/F is a *Galois extension* if it is finite, normal and separable.

Definition 7.6. Let K/F be a Galois extension of fields. The *Galois* group of the extension, written $Gal(K/F)$, is the group of all F-automorphisms of K; that is all automorphisms of K which fix all the elements of F.

Theorem 7.7 (Fundamental Theorem of Galois Theory: [4]: Theorem 8.24)**.** *Let K/F be a Galois extension with Galois group G. Then the maps*

$$\begin{aligned} L &\mapsto Gal(K/L), \\ H &\mapsto Fix(H), \end{aligned}$$

are mutually inverse bijections between the set of subfields of K containing F and the set of subgroups of G.

Moreover, if L_1 and L_2 are intermediate fields, then

$$L_1 \subseteq L_2 \quad \text{if and only if} \quad Gal(K/L_2) \subseteq Gal(K/L_1).$$

Definition 7.8. Let D be an integral domain.

Then denote by $\mathcal{F}(D)$ the *field of fractions* of the domain D so that $\mathcal{F}(D)$ is the smallest field containing D, that is

$$\mathcal{F}(D) = \{\delta_1/\delta_2 \mid \delta_1, \delta_2 \in D, \delta_2 \neq 0\}.$$

Lemma 7.9. *Let R_0 and R_c be the rings as defined in Lemma 7.4 and let $K_0 = \mathcal{F}(R_0)$ and $K_c = \mathcal{F}(R_c)$ so that*

$$K_0 = \mathbb{F}_3(\xi_0, \xi_1, \xi_2, d_3, d_2)$$

and

$$K_c = \mathbb{F}_3(c_3, c_2, c_1, c_0).$$

Then with $S = \mathbb{F}_3[x_1, x_2, x_3, x_4]$ let

$$K = \mathcal{F}(S) = \mathbb{F}_3(x_1, x_2, x_3, x_4)$$

and let G be the Orthogonal group of the quadratic form $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ that is

$$G = O(\xi_0) = O(x_1^2 + x_2^2 + x_3^2 + x_4^2).$$

Then K_0 is the fixed field of the orthogonal group, that is $K_0 = K^G$.

Proof. We have seen that each of the polynomials ξ_0, ξ_1, ξ_2, d_3 and d_2 are invariants of $O(\xi_0)$ so that $K_0 \subseteq K^G$ and we have $R_c \subseteq R_0$ by Lemma 7.4 so that $K_c \subseteq K_0$. Thus we have

$$K_c \subseteq K_0 \subseteq K^G \subseteq K.$$

Now $GL(4,3)$ is the Galois group of the field extension K/K_c by [21] Proposition 8.1.4. By the Fundamental Theorem of Galois Theory: Theorem 7.7, each of the subgroups of $GL(4,3)$ corresponds to a subfield of K containing K_c and so in particular K_0 and K^G correspond to some subgroup of $GL(4,3)$.

Let the subgroup of $GL(4,3)$ corresponding to K_0 be H that is let $H = Gal(K/K_0)$. By hypothesis the subgroup corresponding to K^G is $G = O(\xi_0)$. Now

$$K_0 \subseteq K^G \quad \text{if and only if} \quad Gal(K/K^G) \subseteq Gal(K/K_0)$$

by Theorem 7.7 we have $G \subseteq H$. However, as H is the Galois group of the extension K/K_0 and K_0 the fixed field of H each $h \in H$ fixes $\xi_0 \in K_0$ and so $h \in G$. Thus $H \subseteq G$ and so we see that $H = G$ and thus it follows that $K_0 = K^G$. □

We now proceed to prove that $R_0 = S^G$ and in preparation present the following theory.

Definition 7.10. A *Noetherian domain* is an integral domain in which all ideals are finitely generated.

Theorem 7.11 (Hilbert's Basis Theorem: [1] Theorem 7.5)**.** *Let R be a Noetherian ring then the polynomial ring $R[x]$ is also Noetherian.*

Corollary 7.12. *If R is a Noetherian ring then the polynomial ring $R[x_1, \ldots, x_n]$ is also Noetherian.*

Proof. By induction on n from Theorem 7.11. □

We present the following Lemma which we will use to prove that $R_0 = S^G$.

Lemma 7.13. *Let $R_1 \subseteq R_2$ be commutative Noetherian domains such that*

(i) $\mathcal{F}(R_1) = \mathcal{F}(R_2)$

(ii) R_2 *is a finitely generated* R_1*-module*

(iii) R_1 *is integrally closed.*

Then $R_1 = R_2$.

Proof. Let $y \in R_2$. Then

$$M = \sum_{i \geq 0} R_1 y^i \subseteq R_2.$$

Now since R_1 is Noetherian and as R_2 is a finitely generated R_1-module so R_2 is a Noetherian R_1-module. Thus M is finitely generated R_1-module and so there exists $m \geq 1$ such that

$$M = \sum_{i \geq 0}^{m} R_1 y^i.$$

Thus

$$y^{m+1} = \sum_{i=0}^{m} r_i y^i \qquad \text{for some } r_i \in R_1.$$

Thus y is integral over R_1 as y is a root of the polynomial

$$f(X) = X^{m+1} - \sum_{i=0}^{1} r_1 X^i.$$

Now $y \in \mathcal{F}(R_2) = \mathcal{F}(R_1)$ and so since R_1 is integrally closed it follows that $y \in R_1$ and so $R_2 \subseteq R_1$ and hence $R_1 = R_2$. □

Lemma 7.14 ([3]: Theorem 1.3.1)**.** *Let K be a field and A be a f.g. commutative K-algebra for example $A = K[V]$. Then let G be a finite group of automorphisms of A. Then A^G, the ring of invariants of A under the action of G, is also a f.g. commutative K-algebra and A is finitely generated as a module over A^G.*

Lemma 7.15. *Let the ring $R_0 = \mathbb{F}_3\langle\xi_0, \xi_1, \xi_2, d_3, d_2\rangle$ be as defined in Equation 7.5 and let $S = \mathbb{F}_3[x_1, x_2, x_3, x_4]$. Then S is a finitely generated R_c module.*

Proof. Let R_c be the ring as defined in Lemma 7.4 so that $R_c = S^L$ where $L = GL(4, 3)$ by Lemma 3.2. Then as S is a finitely generated commutative algebra over the field $\mathbb{F}_3$ and L a finite group of automorphisms of S we have that S is finitely generated as a module over $R_c = S^L$ by Lemma 7.14.

In the proof of Lemma 7.4 we observed that $c_i \in R_0$ for $c = 0, \ldots, 3$. Thus if S is finitely generated as a module over R_c then so too must S be finitely generated as a module over R_0. □

Lemma 7.16 ([3]:Proposition 1.21)**.** *A module M over a Noetherian ring is Noetherian if and only if M is finitely generated.*

Corollary 7.17 ([3]:Corollary 1.22)**.** *A submodule of a finitely generated module over a Noetherian ring is finitely generated.*

Lemma 7.18. *Let $S = \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and G be the Orthogonal group $O(x_1^2 + x_2^2 + x_3^2 + x_4^2)$. Then let $R = S^G$ and R_0 be the ring $\mathbb{F}_3\langle\xi_0, \xi_1, \xi_2, d_3, d_2\rangle$ defined in Equation 7.5. Then R is a finitely generated R_0-module.*

Proof. We have

$$R_0 \subseteq R = S^G \subseteq S = \mathbb{F}_q[x_1, x_2, \ldots, x_n].$$

Now

- R_0 is a finitely generated over $\mathbb{F}_3$ and so Noetherian by Theorem 7.11 (HBT),
- S is a finitely generated R-module by Lemma 7.14 and so is a finitely generated module over a Noetherian ring.

Thus R is f.g. R_0-module by Corollary 7.15 being a sub module of a finitely generated module over a Noetherian ring. □

Definition 7.19. Let D be an integral domain. Then the domain D is *integrally closed* if and only if whenever $d \in \mathcal{F}(D)$ is such that d is the root of a monic polynomial with coefficients in D then $d \in D$.

In order to prove that the ring R_0 is the ring of invariants S^G we proceed to show that R_0 is integrally closed.

Lemma 7.20. *If D is a Unique Factorisation Domain then D is integrally closed.*

Proof. Let D be a UFD with $\mathcal{F}(D)$ the field of fractions of D. Then each $f \in \mathcal{F}(D)$ can be expressed as $\frac{f_1}{f_2}$ where $f_1, f_2 \in D$ and f_1 and f_2 have no common factor. If $f \in \mathcal{F}(D)$ is integral over D then for some $m \in \mathbb{N}$ and $a_i \in D$

$$f^m + a_1 f^{m-1} + a_2 f^{m-2} + \cdots + a_{m-1} f = 0.$$

Thus

$$\left(\frac{f_1}{f_2}\right)^m + a_1 \left(\frac{f_1}{f_2}\right)^{m-1} + a_2 \left(\frac{f_1}{f_2}\right)^{m-2} + \cdots + a_{m-1} \frac{f_1}{f_2} = 0$$

and multiplying through by f_2^m

$$f_1^m + a_1 f_1^{m-1} f_2 + a_2 f_1^{m-2} f_2^2 + \cdots + a_{m-1} f_1 {f_2}^{m-1} = 0$$

and so

$$f_1^m = -f_2 \left(a_1 f_1^{m-2} f_2 + a_2 f_1^{m-3} f_2^2 + \cdots + a_{m-1} {f_2}^{m-1}\right).$$

Then as D is UFD f_2 must divide f_1 and since f_1 and f_2 have no common factor $f_2 = \pm 1$.

Thus $f \in D$ and so D is integrally closed. □

Lemma 7.21. *Let T be an integral domain containing an element α such that $T[\alpha^{-1}]$ is UFD and $T/(\alpha)$ is an integral domain.*

Then T is UFD and hence integrally closed by Lemma 7.20.

Proof. The Lemma is a special case of [13] Proposition 1.1. □

Lemma 7.22. *Let R_0 be the sub ring of $S = \mathbb{F}_3[x_1, x_2, x_3, x_4]$ defined in Equation 7.5.*

Then R_0 is integrally closed.

Proof. Let

$$T = \mathbb{F}_3[s_0, s_1, s_2, t_3, t_2]/(\rho)$$

be the polynomial ring where ρ is the relation given in Lemma 7.2.

Denote by $\hat{s_i}$ the image of s_i in T, that is $\hat{s_i} = s_i + (\rho)$.

We see that the relation

$$\rho = -t_2(s_0^3) + t_3(s_1 s_0^4 + s_1^3) - s_0^{11}s_1^2 - s_0^7 s_1^4 + s_0^{10}s_2 + s_0^3 s_1^6 - s_0^6 s_1^2 s_2 - s_0^2 s_1^4 s_2 + s_0 s_1^2 s_2^2 + s_2^3$$

is irreducible as ρ is linear as a polynomial in t_2 and the coefficient $-s_0^3$ of t_2 does not divide the other terms.

With reference to Lemma 7.21 we choose $\alpha = \hat{s_0}$ and consider the localisation $T[\hat{s_0}^{-1}]$ of T.

Now

$$T[\hat{s_0}^{-1}] = \mathbb{F}_3[\hat{s_0}, \hat{s_0}^{-1}, \hat{s_1}, \hat{s_2}, \hat{t_3}]$$

as the relation ρ enables us to express $\hat{t_2}$ in terms of $\hat{s_0}, \hat{s_1}, \hat{s_2}, \hat{t_3}$ together with $\hat{s_0}^{-1}$ and so to eliminate $\hat{t_2}$ from the generators of the ring.

Note that the images of s_0, s_1, s_2, t_3 in T are algebraically independent as the only relations imposed on T are multiples of ρ. Hence the sub algebra U of T generated by the images of s_0, s_1, s_2, t_3 is a polynomial algebra. But $U\langle\hat{s_0}^{-1}\rangle = T\langle\hat{s_0}^{-1}\rangle$ since $\hat{t_2} \in U\langle\hat{s_0}^{-1}\rangle$.

Thus we see that $T[\hat{s_0}^{-1}]$ is UFD being a localisation of a polynomial ring.

We observe that the integral domain

$$\begin{aligned} T/(\hat{s_0}) = T/(s_0 + (\rho)) &= \mathbb{F}_3[s_0, s_1, s_2, t_3, t_2]/\langle s_0, \rho\rangle \\ &= \mathbb{F}_3[s_1, s_2, d_3, d_2]/(\rho_0) \end{aligned}$$

where $\rho_0 = s_2^3 + d_3 s_1^3$ is computed by setting $s_0 = 0$ in the relation ρ.

The relation ρ_0 is irreducible as ρ_0 is linear in d_3 and the coefficient s_1^3 of d_3 does not divide the other term s_2^3.

Then we have that

$$\mathbb{F}_3[s_1, s_2, d_3, d_2]/(\rho_0)$$

is an integral domain being a commutative ring modulo a prime ideal and thus so too is $T/\hat{s_0} = T/(s_0 + (\rho))$ an integral domain.

Thus we see that as T is UFD and so integrally closed by Lemma 7.21 then so too is R_0 integrally closed as $R_0 \cong T$ by Lemma 7.3. □

We can now prove that the ring R_0 is the ring of invariants $\mathbb{F}_3[x_1, x_2, x_3, x_4]^{O(\xi_0)}$.

Theorem 7.23. *Let S be the ring $\mathbb{F}_3[x_1, x_2, x_3, x_4]$ and R_0 be the ring $\mathbb{F}_3\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle \subseteq S$ defined in Equation 7.5.*

Then let G be the orthogonal group of the quadratic form $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Then the ring R_0 is the ring of invariants S^G.

Proof. We have seen that the commutative domain R_0 is Noetherian in the proof of Lemma 7.18. The ring S^G is a finitely generated commutative $\mathbb{F}_3$-algebra by Lemma 7.14 and so is Noetherian. Then we have

(i) $\mathcal{F}(R_0) = \mathcal{F}(S^G)$ by Lemma 7.9,

(ii) R is a finitely generated R_0-algebra by Lemma 7.18 and

(iii) R_0 is integrally closed by Lemma 7.22.

So we see that R_0 and S^G satisfy the hypotheses of Lemma 7.13 taking R_1 as R_0 and R_2 as S^G. Hence, by Lemma 7.13, we have that $R_0 = S^G$ as required. □

Thus we have calculated the ring of invariants of the Orthogonal group $O^+(4, 3)$ as

$$R_0 = \mathbb{F}_3\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle.$$

Chapter 8

Conjectures for greater q and n

8.1 Conjectures in the case $n = 4$

In the previous chapter we were able to present an explicit presentation of the ring of invariants of the Orthogonal group $O(\xi_0)$ in the case $n = 4$, $q = 3$ and $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ of plus type so that in this case $O(\xi_0) \cong O^+(4, 3)$.

Thus we have

$$\mathbb{F}_3[x_1, x_2, x_3, x_4]^{O^+(4,3)} = R_0,$$

where

$$R_0 = \mathbb{F}_3\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle$$

is defined in Equation 7.5, and we have shown there to be one relation ρ on the set of generators where

$$\rho = -d_2(\xi_0^3) + d_3(\xi_1\xi_0^4 + \xi_1^3) - \xi_0^{11}\xi_1^2 - \xi_0^7\xi_1^4 + \xi_0^{10}\xi_2 + \xi_0^3\xi_1^6 - \xi_0^6\xi_1^2\xi_2 - \xi_0^2\xi_1^4\xi_2 + \xi_0\xi_1^2\xi_2^2 + \xi_2^3.$$

We observe that the generators are of degree 2, $q + 1$, $q^2 + 1$, $q^2(q - 1)$ and $(q + 1)q(q - 1)$ and the relation of degree $q(q^2 + 1)$ so that the product of the order of the generators is

$$2 \cdot (q + 1) \cdot (q^2 + 1) \cdot q^2(q - 1) \cdot (q + 1)q(q - 1)$$

Using the formula given in Lemma 2.28 for the order of the Orthogonal groups we see that the Orthogonal group $O^+(4, q)$ has order

$$2q^2(q^2 - 1)^2 = 2q^2(q - 1)^2(q + 1)^2$$

which we note is equal to the product of the degrees of the generators divided by the degree of the relation as we would expect.

On this basis we propose the following conjecture.

Conjecture 8.1. Let V be a vector space of dimension 4 over a finite field of odd characteristic and ξ_0 be a non-singular quadratic form in $S^2(V^*)$, the symmetric square of the dual of V, such that ξ_0 is of plus type as defined in the statement of Lemma 2.18. Then let ξ_1 and ξ_2 be determined from the form ξ_0 by means of the Steenrod operations as presented in §3.2 and d_3 and d_2 be the forms as defined implicitly in the equation

$$d_i^q = c_{4,i} + \phi_i$$

where $c_{4,i}$ is the ith Dickson invariant and ϕ_i is a polynomial in ξ_0, ξ_1, ξ_2 and ξ_3 as detailed in Conjecture 4.1.

Then the ring of invariants of the Orthogonal group is

$$\mathbb{F}_q[x_1, x_2, x_3, x_4]^{O^+(4,q)} = \mathbb{F}_q\langle \xi_0, \xi_1, \xi_2, d_3, d_2 \rangle$$

and there is one relation on the generators of the ring.

The generators then have degree 2, $q+1$, q^2+1, $q^2(q-1)$ and $(q+1)q(q-1)$ and the relation has degree $q(q^2+1)$.

For the case $n = 4$ and ξ_0 is of minus type we have that the Orthogonal group has order

$$2q^2(q^2+1)(q^2-1)$$

from Lemma 2.28.

Thus we see that

$$|O^-(4,q)| = 2 \cdot (q+1) \cdot (q^2+1) \cdot q^2(q-1)$$

so that $|O^-(4,q)|$ is a multiple of the product of the degrees of ξ_0, ξ_1 and ξ_2. In the case $q = 3$ we have seen that there is a Chern Orbit Class of degree $q^2(q-1)$, the remaining factor of $|O^-(4,q)|$, that cannot be written in terms of the forms ξ_k and we have conjectured that there is an invariant d_3 of degree $q^2(q-1)$ in Lemma 4.1.

Thus we are motivated to propose the following conjecture.

Conjecture 8.2. Let V be a vector space of dimension 4 over a finite field of odd characteristic and ξ_0 be a non-singular quadratic form in $S^2(V^*)$, the symmetric square of the dual of V, such that ξ_0 is of minus type as defined in the statement of Lemma 2.18. Then let ξ_1 and ξ_2 be determined from the form ξ_0 by means of the Steenrod operations as presented in §3.2 and d_3 be the form defined implicitly in the equation

$$d_3^q = c_{4,3} + \phi_3$$

where $c_{4,3}$ is a Dickson invariant and ϕ_i is a polynomial in ξ_0, ξ_1, ξ_2 and ξ_3.

Then the ring of invariants of the Orthogonal group is a polynomial ring and moreover

$$\mathbb{F}_q[x_1, x_2, x_3, x_4]^{O^-(4,q)} = \mathbb{F}_q[\xi_0, \xi_1, \xi_2, d_3].$$

8.2 Considering the cases $n = 2$ and $n = 3$

In §4.5 we proposed that, in the case $n = 3$, the ring of invariants of the Orthogonal group $O(\xi_0)$ is

$$\mathbb{F}_q[x_1, x_2, x_3]^{O(3,q)} = \mathbb{F}_q[\xi_0, \xi_1, d_2]$$

where $d_2^q = c_{3,2} + \phi_2$ for ϕ_2 a polynomial in the ξ_k.

We consider the order of the Orthogonal group $O(3, q)$ with reference to Lemma 2.28 and observe that

$$|O(3, q)| = 2q(q^2 - 1) = 2 \cdot (q + 1) \cdot q(q - 1)$$

which is equal to the product of the degrees of ξ_0, ξ_1 and $c_{3,2}$ as we expect. We note that this is consistent with Conjecture 4.4.

In the case $n = 2$ we have

$$|O(^+2, q)| = 2(q - 1) \quad \text{and} \quad |O(^-2, q)| = 2(q + 1).$$

We have proved in Theorem 4.2 that there exists an invariant d_1 of degree $q - 1$ such that $d_1^q = c_{2,1} + \phi_1$ for ϕ_1 a polynomial in the ξ_k when ξ_0 is a quadratic form of plus type but for ξ_0 of minus type no such invariant exists as $d_1 = 0$.

Thus we propose that

$$\mathbb{F}_q[x_1, x_2]^{O^+(2,q)} = \mathbb{F}_q[\xi_0, d_1]$$

and

$$\mathbb{F}_q[x_1, x_2]^{O^-(2,q)} = \mathbb{F}_q[\xi_0, \xi_1].$$

8.3 The ring of invariants of the Orthogonal group in higher dimensions

We consider first the case when $n = 2s + 1$ and have in this case by Lemma 2.28

$$\begin{aligned} |O(n,q)| &= 2q^{s^2} \prod_{i=1}^{s} (q^{2i} - 1) \\ &= 2q^{s^2} \prod_{i=1}^{s} (q^i + 1)(q^i - 1) \\ &= \prod_{i=0}^{s} (q^i + 1) \cdot q^{s^2} \prod_{i=1}^{s} (q^i - 1). \end{aligned}$$

Thus we expect to have among the generators $\xi_0, \xi_1, \ldots \xi_s$ and $d_{n-1}, d_{n-2}, \ldots, d_{n-s}$ as the product of the degrees of these is

$$\begin{aligned} \prod_{i=0}^{s} (q^i + 1) \cdot \prod_{i=1}^{s} \frac{(q^n - q^{n-i})}{q} &= \prod_{i=0}^{s} (q^i + 1) \cdot \prod_{i=1}^{s} q^{2s-i}(q^i - 1) \\ &= \prod_{i=0}^{s} (q^i + 1) \cdot q^m \prod_{i=1}^{s} (q^i - 1) \end{aligned}$$

where $m = \frac{s(3s-1)}{2} \geq s^2$ for $s \geq 1$.

For example in the case $n = 5$ we might expect one relation as there we propose none in the case $n = 3$.

Thus we propose the ring of invariants in the case $n = 5$ as

$$\mathbb{F}_q[x_1, \ldots, x_5]^{O(5,q)} = \mathbb{F}_q\langle \xi_0, \xi_1, \xi_2, \xi_3, d_4, d_3 \rangle$$

with a relation of degree $q(q^3 + 1)$.

Secondly we consider the case $n = 2s$ and have from Lemma 2.28 that

$$\begin{aligned} |O^+(n,q)| &= 2q^{s(s-1)}(q^s-1)\prod_{i=1}^{s-1}(q^{2i}-1) \\ &= 2q^{s(s-1)}(q^s-1)\prod_{i=1}^{s-1}(q^i+1)(q^i-1) \\ &= \prod_{i=0}^{s-1}(q^i+1)\cdot q^{s(s-1)}\prod_{i=1}^{s}(q^i-1). \end{aligned}$$

Again we expect to have amongst the generators ξ_0, ξ_1, ξ_1 and $d_{n-1}, \ldots, d_{n-s}$.

For example in the case $n = 6$ the product of the degrees of ξ_0, ξ_1, ξ_2 and $d_{n-1}, \ldots, d_{n-s}$ being

$$\prod_{i=0}^{s-1}(q^i+1)\cdot q^9\prod_{i=1}^{s}(q^i-1)$$

so that the product of the degrees of the relations must be a multiple of q^3. We would expect 2 relations in this case as there was 1 in the case $n = 4$.

Thus we might propose that the ring of invariants

$$\mathbb{F}_q[x_1, \ldots, x_5]^{O^+(6,q)} = \mathbb{F}_q\langle \xi_0, \xi_1, \ldots, \xi_4, d_5, d_4, d_3, d_2\rangle$$

with 2 relations the product of their degrees being $q^3(q^4+1)(q^3+1) = q(q^4+1)\cdot q^2(q^3+1)$.

By a similar argument we might propose that the ring invariants

$$\mathbb{F}_q[x_1, \ldots, x_5]^{O^-(6,q)} = \mathbb{F}_q\langle \xi_0, \xi_1, \ldots, \xi_4, d_5, d_4\rangle$$

with relation of degree $q(q^4+1)$.

We can hope to generalise the above proposals by consideration of the order of the Orthogonal groups. Verification of any such conjectures are hard to validate using CoCoA code as above the case for $n = 4$ and $q = 3$ the calculations become large. However, we believe that it is possible to consider some more cases by calculation with some increased computer power so that with this greater insight an understanding of the full picture might be achieved.

Appendix A

Investigating the chern orbits classes

We present CoCoA code ascertaining which of the Chern orbit cannot be written as a polynomial in the ξ_k's.

A.1 CoCoA code in the case $n = 3$

First we present the code for the ξ_k and the Chern Orbit Polynomials procedures.

- ChCo(K): generates the Chern Polynomial for vectors in V^* corresponding to a vector in V on which the form is equal to k.
- Xi(K): generates the form ξ_k.

```
Define ChCo(K)
    N:=MEMORY.N; P:=MEMORY.P; Ep:=MEMORY.Ep; Ch:=1;
    For A1:=0 To P-1 Do For A2:=0 To P-1 Do For A3:=0 To P-1 Do
        If Not A1=0 And A2=0 And A3=0 Then Xi:=Ep*A1^2+A2^2+A3^2;
            If Mod(Xi,P)=K Then X:=Ep*A1*x[1]+A2*x[2]+A3*x[3]; Ch:=Ch*(t-X);
    EndIf EndIf EndFor EndFor EndFor;
    ChCo:=Coefficients(Ch,t);
Return ChCo; EndDefine;

Define Xi(K) N:=MEMORY.N; P:=MEMORY.P; Ep:=MEMORY.Ep; Xi:=Ep*x[1]^(P^K+1);
For J:=2 To N Do Xi:=Xi+x[J]^(P^K+1) EndFor;
Return Xi EndDefine;
```

The following procedures are used to generate a matrix of coefficients of a system of forms of a given degree and to reduce the matrix to row-reduced echelon form.

- PXi(D): generates a list of possible combinations of powers of ξ_2, ξ_1 and ξ_0 in expressions of a given degree.
- RoCo(Pol): generates a list of coefficients of a given form in 3 indeterminates including zero coefficients.
- RRM(A): reduces a matrix to row-reduced echelon form working if the field Z/p where p is prime.
- XiSol(Pol): produces, for a given form of degree D, a matrix, Mm whose rows are the coefficients of each possible form of D in powers of ξ_2, ξ_1, ξ_0 and whose final row is the coefficients of the given form.

  The transpose of this matrix, Mm, is then reduced to row-reduced echelon form and the zero rows removed.

  The final column of the matrix is then use along with Pxi(Pol) to return 'Pol' as a polynomial in the ξ_k's if possible or to return that no possible solution can be found if that is the case.

```
Define PXi(D) P:=MEMORY.P;
    M2:=Div(D,(P^2+1)); C:=0;
    For D2:=M2 To 0 Step -1 Do
        M1:=Div(D-D2*(P^2+1),(P+1)); C:=C+M1+1;
    EndFor;
    M:=NewList(C);C1:=0; Mm:=NewList(C);
    For D2:=M2 To 0 Step -1 Do
        M1:=Div(D-D2*(P^2+1),(P+1));
        For D1:=M1 To 0 Step -1 Do
            D0:=(D-D2*(P^2+1)-D1*(P+1))/2;
            C1:=C1+1; M[C1]:=[D2,D1,D0];
    EndFor; EndFor;
    Return M;
EndDefine;
```

```
Define RoCo(Pol);
    D:=Deg(Pol); If D=0 Then Return 'Pol is constant' Else
    Nt:=(D+1)*(D+2)/2; Rc:=NewList(Nt);
    E1:=NewList(D+1); D1:=Log(Pol); Dif1:=D-D1[1]+1;
    Pol:=Subst(Pol,x[3],1); Cx1:=Coefficients(Pol,x[1]);
        For J1:=1 To D+1 Do E2:=NewList(J1);
            If J1<Dif1 Then E1[J1]:=0 Else E1[J1]:=Cx1[J1-Dif1+1] EndIf;
            If E1[J1]=0 Then For J2:=1 To J1 Do E2[J2]:=0 EndFor;
            Else Cx2:=Coefficients(E1[J1],x[2]); D2:=Log(E1[J1]); Dif2:=J1-D2[2]-1;
                For J2:=1 To J1 Do
                    If J2<=Dif2 Then E2[J2]:=0 Else E2[J2]:=Cx2[J2-Dif2] EndIf;
            EndFor; EndIf; E1[J1]:=E2;
        EndFor; C:=1;
        For J1:=1 To D+1 Do For J2:=1 To J1 Do
            Rc[C]:=E1[J1,J2]; C:=C+1
        EndFor;EndFor;
Return Rc; EndIf; EndDefine;

Define RRM(A) C:=Len(A[1]); R:=Len(A); If C>R Then PrintLn 'Error C>R' EndIf;
    Min:=C; --As C is less than R
    For I:=1 To Min-1 Do If A[I,I]=0 Then
        For K:=I+1 To R Do If A[K,I]<>0 Then
             Ae:=A[I]; A[I]:=A[K]; A[K]:=Ae; Break
        EndIf EndFor EndIf;
        Dv:=Poly(Inverse(LC(A[I,I]))); A[I]:=Dv*A[I];
        For J:=1 To R Do
            If J<>I Then Mt:=Poly(A[J,I]);A[J]:=A[J]-Mt*A[I]
    EndIf; EndFor;EndFor; A:=List(A);
    For I:=R To Min Step -1 Do If A[I,Min]<>0 Then
        For J:=I-1 To Min Step -1 Do Remove(A,J) EndFor; Break
        Else Remove(A,I);
    EndIf; EndFor; A:=Mat(A);
Return A; EndDefine;
```

```
Define XiSol(Pol)  P:=MEMORY.P; Ep:=MEMORY.Ep;
    If Pol=0 Then PrintLn 'Pol=0' Elsif Deg(Pol)=0 Then PrintLn 'Deg(Pol)=0';
        Else D:=Deg(Pol);
        Xi0:=Xi(0); Xi1:=Xi(1); Xi2:=Xi(2);
        M:=PXi(D); PolCo:=RoCo(Pol);
        PXiR:=NewList(Len(M));
        For K:=1 To Len(M) Do PXiR[K]:=RoCo(Xi2^M[K,1]*Xi1^M[K,2]*Xi0^M[K,3]) EndFor;
        L1:=Len(M); L2:=Len(PolCo);
        Mm:=NewMat(L1+1,L2); Mm[L1+1]:=PolCo;
        For I:=1 To L1 Do Mm[I]:=PXiR[I] EndFor;
        N:=Transposed(Mm); RRMN:=RRM(N);
        If Len(RRMN)=Len(RRMN[1]) Then Return 'Not'; Else Sol:=0;
        For I:=1 To Len(M) Do
            Term:= RRMN[I,Len(M)+1]*s[2]^M[I,1]*s[1]^M[I,2]*s[0]^M[I,3];
            Sol:=Sol+Term
        EndFor;
Return Sol EndIf EndIf EndDefine;
```

We now implement the algorithm for the case $n = 3$, $q = 3$ and $\xi_0 = Q_s = x_1^2 + x_2^2 + x_3^2$ or $\xi_0 = Q_n = \varepsilon x_1^2 + x_2^2 + x_3^2$ for ε a non square in $\mathbb{F}_q^*$ investigating all the Chern orbit classes of the Chern polynomial when for $k = 0$.

```
N:=3; MEMORY.N:=N; P:=3; MEMORY.P:=P; N1:=N-1; Ep:=1; MEMORY.Ep:=Ep;
Use R::=Z/(P)[x[1..N],s[0..N1],t];
PrintLn;Print 'N=',N,' P=',P,' Ep=',Ep;
Print 'Expect new invariants of degree ',(P^N-P^2)/P;
For J:=0 To 0 Do PrintLn; PrintLn 'ChCo(',J,')'; ChCo:=ChCo(J);
    If ChCo=1 Then PrintLn 'ChCo(',J,') is 1' Else
        For I:=P To Len(ChCo) Step P-1 Do XiMat:=XiMat(ChCo[I]);
            If XiMat='Not' Then PrintLn 'The chern orbit class of degree ',Deg(ChCo[I]),'
                cannot be written as a polynomial in the xis'
            Elsif XiMat=Null Then
            PrintLn 'The chern coefficient is of degree ',Deg(ChCo[I])
            Else PrintLn 'The Chern coefficient of degree ',Deg(ChCo[I]),' is ', XiMat
EndIf EndFor EndIf EndFor;
```

A.2 Output when n=3

Here we present the output of the code of the previous section for $n = 3$, $q = 3$ and $\xi_0 = Q_s$ when $\varepsilon = 1$ and $\xi_0 = Q_n$ when ε is a non-square in $\mathbb{F}_q^*$.

```
N=3 P=3 Ep=1  Expect new invariants of degree 6
ChCo(0)
Degree of poly is 9
The Chern coefficient of degree 2 is -s[0]
The Chern coefficient of degree 4 is -s[0]^2 + s[1]
The chern coefficient of degree 6 cannot be written as a polynomial in the xis
The Chern coefficient of degree 8 is s[0]^4 - s[0]^2s[1] + s[1]^2
------------------------------
N=3 P=3 Ep=2  Expect new invariants of degree 6
ChCo(0)
Degree of poly is 9
The Chern coefficient of degree 2 is s[0]
The Chern coefficient of degree 4 is -s[0]^2 - s[1]
The chern coefficient of degree 6 cannot be written as a polynomial in the xis
The Chern coefficient of degree 8 is s[0]^4 + s[0]^2s[1] + s[1]^2
------------------------------
N=3 P=5 Ep=1  Expect new invariants of degree 20
ChCo(0)
Degree of poly is 25
The Chern coefficient of degree 4 is s[0]^2
The Chern coefficient of degree 8 is -2s[0]^4 - 2s[0]s[1]
The Chern coefficient of degree 12 is -2s[0]^3s[1] - 2s[1]^2
The Chern coefficient of degree 16 is -2s[0]^8 - 2s[0]^5s[1]
The chern coefficient of degree 20 cannot be written as a polynomial in the xis
The Chern coefficient of degree 24
                  is s[0]^12 + s[0]^9s[1] + s[0]^6s[1]^2 + s[0]^3s[1]^3 + s[1]^4
------------------------------
N=3 P=5 Ep=2  Expect new invariants of degree 20
ChCo(0)
Degree of poly is 25
The Chern coefficient of degree 4 is -s[0]^2
```

```
The Chern coefficient of degree 8 is -2s[0]^4 + 2s[0]s[1]
The Chern coefficient of degree 12 is -2s[0]^3s[1] + 2s[1]^2
The Chern coefficient of degree 16 is -2s[0]^8 + 2s[0]^5s[1]
The chern coefficient of degree 20 cannot be written as a polynomial in the xis
The Chern coefficient of degree 24
                is s[0]^12 - s[0]^9s[1] + s[0]^6s[1]^2 - s[0]^3s[1]^3 + s[1]^4
-------------------------------
N=3 P=7 Ep=1  Expect new invariants of degree 42
ChCo(0)
Degree of poly is 49
The Chern coefficient of degree 6 is -s[0]^3
The Chern coefficient of degree 12 is -3s[0]^6 + 3s[0]^2s[1]
The Chern coefficient of degree 18 is -3s[0]^5s[1] + 3s[0]s[1]^2
The Chern coefficient of degree 24
               is -s[0]^12 + s[0]^8s[1] - 2s[0]^4s[1]^2 + 2s[1]^3
The Chern coefficient of degree 30 is -3s[0]^11s[1] + 3s[0]^7s[1]^2
The Chern coefficient of degree 36 is -3s[0]^18 + 3s[0]^14s[1]
The chern coefficient of degree 42 cannot be written as a polynomial in the xis
The Chern coefficient of degree 48 is s[0]^24 - s[0]^20s[1] + s[0]^16s[1]^2
                        - s[0]^12s[1]^3 + s[0]^8s[1]^4 - s[0]^4s[1]^5 + s[1]^6
-------------------------------
N=3 P=7 Ep=3  Expect new invariants of degree 42
ChCo(0)
Degree of poly is 49
The Chern coefficient of degree 6 is s[0]^3
The Chern coefficient of degree 12 is -3s[0]^6 - 3s[0]^2s[1]
The Chern coefficient of degree 18 is -3s[0]^5s[1] - 3s[0]s[1]^2
The Chern coefficient of degree 24
               is -s[0]^12 - s[0]^8s[1] - 2s[0]^4s[1]^2 - 2s[1]^3
The Chern coefficient of degree 30 is -3s[0]^11s[1] - 3s[0]^7s[1]^2
The Chern coefficient of degree 36 is -3s[0]^18 - 3s[0]^14s[1]
The chern coefficient of degree 42 cannot be written as a polynomial in the xis
The Chern coefficient of degree 48 is s[0]^24 + s[0]^20s[1] + s[0]^16s[1]^2
                        + s[0]^12s[1]^3 + s[0]^8s[1]^4 + s[0]^4s[1]^5 + s[1]^6
```

A.3 Output when $n = 4$

Similar code to that presented in Appendix A.1 is used for the case $n = 4$ and $q = 3$ and the output given here in the case $q = 3$.

In the first case $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and so is of plus type.

```
------------------------------
N=4 Q=3 Ep=1
------------------------------
Expect new invariants of degree 24
Degree of Chern(0) is 33
Pol=0
Pol=0
The Chern coefficient of degree 6 is -s[0]s[1]
The Chern coefficient of degree 8 is s[0]^4 - s[1]^2
Pol=0
The Chern coefficient of degree 12 is -s[0]^6 - s[0]^2s[1]^2 - s[0]s[2]
The Chern coefficient of degree 14 is -s[0]^5s[1] - s[0]s[1]^3 - s[1]s[2]
The Chern coefficient of degree 16 is -s[0]^8 - s[0]^4s[1]^2 - s[0]^3s[2]
The chern coefficient of degree 18 cannot be written as a polynomial in the xis
The Chern coefficient of degree 20 is -s[0]^5s[2] - s[0]s[1]^2s[2] - s[2]^2
The Chern coefficient of degree 22 is -s[0]^5s[1]^3 - s[0]s[1]^5 - s[1]^3s[2]
The chern coefficient of degree 24 cannot be written as a polynomial in the xis
The Chern coefficient of degree 26 is -s[0]^11s[1] + s[0]^7s[1]^3 + s[0]^3s[1]^5
                                                    - s[0]^6s[1]s[2]
The Chern coefficient of degree 28 is -s[0]^14 - s[0]^10s[1]^2 - s[0]^9s[2]
The chern coefficient of degree 30 cannot be written as a polynomial in the xis
The chern coefficient of degree 32 cannot be written as a polynomial in the xis
------------------------------
```

In the second case $\xi_0 = 2x_1^2 + x_2^2 + x_3^2 + x_4^2$ and so is of minus type.

```
N=4 Q=3 Ep=2
------------------------------
Expect new invariants of degree 18
------------------------------
Degree of Chern(0)  is 21
Pol=0
Pol=0
The Chern coefficient of degree 6 is s[0]s[1]
The Chern coefficient of degree 8 is -s[0]^4 + s[1]^2
Pol=0
The Chern coefficient of degree 12 is s[0]^6 - s[0]^2s[1]^2 + s[0]s[2]
The Chern coefficient of degree 14 is -s[0]^5s[1] + s[1]s[2]
The Chern coefficient of degree 16 is -s[0]^8 - s[0]^4s[1]^2 + s[1]^4 + s[0]^3s[2]
The chern coefficient of degree 18 cannot be written as a polynomial in the xis
The Chern coefficient of degree 20 is s[0]^10 - s[0]^6s[1]^2 + s[0]^2s[1]^4
                                        - s[0]^5s[2] - s[0]s[1]^2s[2] + s[2]^2
------------------------------
```

A.4 The invariants h_3 and h_2 of $O^+(4,3)$

In the case $n = 4$, $q = 3$ and $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ we have calculated the invariants h_3 and h_2 as defined in 3.23 using CoCoA code and we present the invariants explicitly below as H43 and H42 respectively.

```
D43=-x[1]^18 - x[1]^12x[2]^6 - x[1]^6x[2]^12 - x[2]^18 + x[1]^14x[2]^2x[3]^2 - x[1]^10x[2]^6x[3]^2
- x[1]^6x[2]^10x[3]^2 + x[1]^2x[2]^14x[3]^2 - x[1]^10x[2]^4x[3]^4 - x[1]^4x[2]^10x[3]^4
- x[1]^12x[3]^6 - x[1]^10x[2]^2x[3]^6 - x[1]^6x[2]^6x[3]^6 - x[1]^2x[2]^10x[3]^6 - x[2]^12x[3]^6
- x[1]^6x[2]^2x[3]^10 - x[1]^4x[2]^4x[3]^10 - x[1]^2x[2]^6x[3]^10 - x[1]^6x[3]^12 - x[2]^6x[3]^12
+ x[1]^2x[2]^2x[3]^14 - x[3]^18 + x[1]^14x[2]^2x[4]^2 - x[1]^10x[2]^6x[4]^2 - x[1]^6x[2]^10x[4]^2
+ x[1]^2x[2]^14x[4]^2 + x[1]^14x[3]^2x[4]^2 - x[1]^12x[2]^2x[3]^2x[4]^2
- x[1]^10x[2]^4x[3]^2x[4]^2 - x[1]^4x[2]^10x[3]^2x[4]^2 - x[1]^2x[2]^12x[3]^2x[4]^2
+ x[2]^14x[3]^2x[4]^2 - x[1]^10x[2]^2x[3]^4x[4]^2 - x[1]^6x[2]^6x[3]^4x[4]^2
- x[1]^2x[2]^10x[3]^4x[4]^2 - x[1]^10x[3]^6x[4]^2 - x[1]^6x[2]^4x[3]^6x[4]^2
- x[1]^4x[2]^6x[3]^6x[4]^2 - x[2]^10x[3]^6x[4]^2 - x[1]^6x[3]^10x[4]^2 - x[1]^4x[2]^2x[3]^10x[4]^2
- x[1]^2x[2]^4x[3]^10x[4]^2 - x[2]^6x[3]^10x[4]^2 - x[1]^2x[2]^2x[3]^12x[4]^2 + x[1]^2x[3]^14x[4]^2
+ x[2]^2x[3]^14x[4]^2 - x[1]^10x[2]^4x[4]^4 - x[1]^4x[2]^10x[4]^4 - x[1]^10x[2]^2x[3]^2x[4]^4
- x[1]^6x[2]^6x[3]^2x[4]^4 - x[1]^2x[2]^10x[3]^2x[4]^4 - x[1]^10x[3]^4x[4]^4
- x[1]^6x[2]^4x[3]^4x[4]^4 - x[1]^4x[2]^6x[3]^4x[4]^4 - x[2]^10x[3]^4x[4]^4
- x[1]^6x[2]^2x[3]^6x[4]^4 - x[1]^4x[2]^4x[3]^6x[4]^4 - x[1]^2x[2]^6x[3]^6x[4]^4
- x[1]^4x[3]^10x[4]^4 - x[1]^2x[2]^2x[3]^10x[4]^4 - x[2]^4x[3]^10x[4]^4 - x[1]^12x[4]^6
- x[1]^10x[2]^2x[4]^6 - x[1]^6x[2]^6x[4]^6 - x[1]^2x[2]^10x[4]^6 - x[2]^12x[4]^6
- x[1]^10x[3]^2x[4]^6 - x[1]^6x[2]^4x[3]^2x[4]^6 - x[1]^4x[2]^6x[3]^2x[4]^6 - x[2]^10x[3]^2x[4]^6
- x[1]^6x[2]^2x[3]^4x[4]^6 - x[1]^4x[2]^4x[3]^4x[4]^6 - x[1]^2x[2]^6x[3]^4x[4]^6
- x[1]^6x[3]^6x[4]^6 - x[1]^4x[2]^2x[3]^6x[4]^6 - x[1]^2x[2]^4x[3]^6x[4]^6 - x[2]^6x[3]^6x[4]^6
 - x[1]^2x[3]^10x[4]^6 - x[2]^2x[3]^10x[4]^6 - x[3]^12x[4]^6 - x[1]^6x[2]^2x[4]^10
- x[1]^4x[2]^4x[4]^10 - x[1]^2x[2]^6x[4]^10 - x[1]^6x[3]^2x[4]^10 - x[1]^4x[2]^2x[3]^2x[4]^10
- x[1]^2x[2]^4x[3]^2x[4]^10 - x[2]^6x[3]^2x[4]^10 - x[1]^4x[3]^4x[4]^10
- x[1]^2x[2]^2x[3]^4x[4]^10 - x[2]^4x[3]^4x[4]^10 - x[1]^2x[3]^6x[4]^10 - x[2]^2x[3]^6x[4]^10
- x[1]^6x[4]^12 - x[2]^6x[4]^12 - x[1]^2x[2]^2x[3]^2x[4]^12 - x[3]^6x[4]^12 + x[1]^2x[2]^2x[4]^14
 + x[1]^2x[3]^2x[4]^14 + x[2]^2x[3]^2x[4]^14 - x[4]^18
```

```
H42=x[1]^24 + x[1]^22x[2]^2 + x[1]^20x[2]^4 + x[1]^16x[2]^8 + x[1]^14x[2]^10 + x[1]^10x[2]^14
+ x[1]^8x[2]^16 + x[1]^4x[2]^20 + x[1]^2x[2]^22 + x[2]^24 + x[1]^22x[3]^2 + x[1]^20x[2]^2x[3]^2
+ x[1]^18x[2]^4x[3]^2 - x[1]^16x[2]^6x[3]^2 - x[1]^12x[2]^10x[3]^2 - x[1]^10x[2]^12x[3]^2
- x[1]^6x[2]^16x[3]^2 + x[1]^4x[2]^18x[3]^2 + x[1]^2x[2]^20x[3]^2 + x[2]^22x[3]^2 + x[1]^20x[3]^4
+ x[1]^18x[2]^2x[3]^4 - x[1]^16x[2]^4x[3]^4 - x[1]^12x[2]^8x[3]^4 - x[1]^8x[2]^12x[3]^4
- x[1]^4x[2]^16x[3]^4 + x[1]^2x[2]^18x[3]^4 + x[2]^20x[3]^4 - x[1]^16x[2]^2x[3]^6
+ x[1]^12x[2]^6x[3]^6 + x[1]^10x[2]^8x[3]^6 + x[1]^8x[2]^10x[3]^6 + x[1]^6x[2]^12x[3]^6
- x[1]^2x[2]^16x[3]^6 + x[1]^16x[3]^8 - x[1]^12x[2]^4x[3]^8 + x[1]^10x[2]^6x[3]^8
+ x[1]^6x[2]^10x[3]^8 - x[1]^4x[2]^12x[3]^8 + x[2]^16x[3]^8 + x[1]^14x[3]^10 - x[1]^12x[2]^2x[3]^10
+ x[1]^8x[2]^6x[3]^10 + x[1]^6x[2]^8x[3]^10 - x[1]^2x[2]^12x[3]^10 + x[2]^14x[3]^10
- x[1]^10x[2]^2x[3]^12 - x[1]^8x[2]^4x[3]^12 + x[1]^6x[2]^6x[3]^12 - x[1]^4x[2]^8x[3]^12
- x[1]^2x[2]^10x[3]^12 + x[1]^10x[3]^14 + x[2]^10x[3]^14 + x[1]^8x[3]^16 - x[1]^6x[2]^2x[3]^16
- x[1]^4x[2]^4x[3]^16 - x[1]^2x[2]^6x[3]^16 + x[2]^8x[3]^16 + x[1]^4x[2]^2x[3]^18
+ x[1]^2x[2]^4x[3]^18 + x[1]^4x[3]^20 + x[1]^2x[2]^2x[3]^20 + x[2]^4x[3]^20 + x[1]^2x[3]^22
+ x[2]^2x[3]^22 + x[3]^24 + x[1]^22x[4]^2 + x[1]^20x[2]^2x[4]^2 + x[1]^18x[2]^4x[4]^2
- x[1]^16x[2]^6x[4]^2 - x[1]^12x[2]^10x[4]^2 - x[1]^10x[2]^12x[4]^2 - x[1]^6x[2]^16x[4]^2
+ x[1]^4x[2]^18x[4]^2 + x[1]^2x[2]^20x[4]^2 + x[2]^22x[4]^2 + x[1]^20x[3]^2x[4]^2
- x[1]^18x[2]^2x[3]^2x[4]^2 + x[1]^16x[2]^4x[3]^2x[4]^2 + x[1]^14x[2]^6x[3]^2x[4]^2
- x[1]^12x[2]^8x[3]^2x[4]^2 - x[1]^10x[2]^10x[3]^2x[4]^2 - x[1]^8x[2]^12x[3]^2x[4]^2
+ x[1]^6x[2]^14x[3]^2x[4]^2 + x[1]^4x[2]^16x[3]^2x[4]^2 - x[1]^2x[2]^18x[3]^2x[4]^2
+ x[2]^20x[3]^2x[4]^2 + x[1]^18x[3]^4x[4]^2 + x[1]^16x[2]^2x[3]^4x[4]^2 + x[1]^14x[2]^4x[3]^4x[4]^2
- x[1]^10x[2]^8x[3]^4x[4]^2 - x[1]^8x[2]^10x[3]^4x[4]^2 + x[1]^4x[2]^14x[3]^4x[4]^2
+ x[1]^2x[2]^16x[3]^4x[4]^2 + x[2]^18x[3]^4x[4]^2 - x[1]^16x[3]^6x[4]^2 + x[1]^14x[2]^2x[3]^6x[4]^2
+ x[1]^10x[2]^6x[3]^6x[4]^2 - x[1]^8x[2]^8x[3]^6x[4]^2 + x[1]^6x[2]^10x[3]^6x[4]^2
+ x[1]^2x[2]^14x[3]^6x[4]^2 - x[2]^16x[3]^6x[4]^2 - x[1]^12x[2]^2x[3]^8x[4]^2
- x[1]^10x[2]^4x[3]^8x[4]^2 - x[1]^8x[2]^6x[3]^8x[4]^2 - x[1]^6x[2]^8x[3]^8x[4]^2
- x[1]^4x[2]^10x[3]^8x[4]^2 - x[1]^2x[2]^12x[3]^8x[4]^2 - x[1]^12x[3]^10x[4]^2
- x[1]^10x[2]^2x[3]^10x[4]^2 - x[1]^8x[2]^4x[3]^10x[4]^2 + x[1]^6x[2]^6x[3]^10x[4]^2
- x[1]^4x[2]^8x[3]^10x[4]^2 - x[1]^2x[2]^10x[3]^10x[4]^2 - x[2]^12x[3]^10x[4]^2
- x[1]^10x[3]^12x[4]^2 - x[1]^8x[2]^2x[3]^12x[4]^2 - x[1]^2x[2]^8x[3]^12x[4]^2
- x[2]^10x[3]^12x[4]^2 + x[1]^6x[2]^2x[3]^14x[4]^2 + x[1]^4x[2]^4x[3]^14x[4]^2
+ x[1]^2x[2]^6x[3]^14x[4]^2 - x[1]^6x[3]^16x[4]^2 + x[1]^4x[2]^2x[3]^16x[4]^2
+ x[1]^2x[2]^4x[3]^16x[4]^2 - x[2]^6x[3]^16x[4]^2 + x[1]^4x[3]^18x[4]^2 - x[1]^2x[2]^2x[3]^18x[4]^2
+ x[2]^4x[3]^18x[4]^2 + x[1]^2x[3]^20x[4]^2 + x[2]^2x[3]^20x[4]^2 + x[3]^22x[4]^2 + x[1]^20x[4]^4
+ x[1]^18x[2]^2x[4]^4 - x[1]^16x[2]^4x[4]^4 - x[1]^12x[2]^8x[4]^4 - x[1]^8x[2]^12x[4]^4
- x[1]^4x[2]^16x[4]^4 + x[1]^2x[2]^18x[4]^4 + x[2]^20x[4]^4 + x[1]^18x[3]^2x[4]^4
+ x[1]^16x[2]^2x[3]^2x[4]^4 + x[1]^14x[2]^4x[3]^2x[4]^4 - x[1]^10x[2]^8x[3]^2x[4]^4
- x[1]^8x[2]^10x[3]^2x[4]^4 + x[1]^4x[2]^14x[3]^2x[4]^4 + x[1]^2x[2]^16x[3]^2x[4]^4
```

```
+ x[2]^18x[3]^2x[4]^4 - x[1]^16x[3]^4x[4]^4 + x[1]^14x[2]^2x[3]^4x[4]^4 - x[1]^12x[2]^4x[3]^4x[4]^4
- x[1]^10x[2]^6x[3]^4x[4]^4 - x[1]^8x[2]^8x[3]^4x[4]^4 - x[1]^6x[2]^10x[3]^4x[4]^4
- x[1]^4x[2]^12x[3]^4x[4]^4 + x[1]^2x[2]^14x[3]^4x[4]^4 - x[2]^16x[3]^4x[4]^4
- x[1]^10x[2]^4x[3]^6x[4]^4 + x[1]^8x[2]^6x[3]^6x[4]^4 + x[1]^6x[2]^8x[3]^6x[4]^4
- x[1]^4x[2]^10x[3]^6x[4]^4 - x[1]^12x[3]^8x[4]^4 - x[1]^10x[2]^2x[3]^8x[4]^4
- x[1]^8x[2]^4x[3]^8x[4]^4 + x[1]^6x[2]^6x[3]^8x[4]^4 - x[1]^4x[2]^8x[3]^8x[4]^4
- x[1]^2x[2]^10x[3]^8x[4]^4 - x[2]^12x[3]^8x[4]^4 - x[1]^8x[2]^2x[3]^10x[4]^4
- x[1]^6x[2]^4x[3]^10x[4]^4 - x[1]^4x[2]^6x[3]^10x[4]^4 - x[1]^2x[2]^8x[3]^10x[4]^4
- x[1]^8x[3]^12x[4]^4 - x[1]^4x[2]^4x[3]^12x[4]^4 - x[2]^8x[3]^12x[4]^4 + x[1]^4x[2]^2x[3]^14x[4]^4
+ x[1]^2x[2]^4x[3]^14x[4]^4 - x[1]^4x[3]^16x[4]^4 + x[1]^2x[2]^2x[3]^16x[4]^4
- x[2]^4x[3]^16x[4]^4 + x[1]^2x[3]^18x[4]^4 + x[2]^2x[3]^18x[4]^4 + x[3]^20x[4]^4
- x[1]^16x[2]^2x[4]^6 + x[1]^12x[2]^6x[4]^6 + x[1]^10x[2]^8x[4]^6 + x[1]^8x[2]^10x[4]^6
+ x[1]^6x[2]^12x[4]^6 - x[1]^2x[2]^16x[4]^6 - x[1]^16x[3]^2x[4]^6 + x[1]^14x[2]^2x[3]^2x[4]^6
+ x[1]^10x[2]^6x[3]^2x[4]^6 - x[1]^8x[2]^8x[3]^2x[4]^6 + x[1]^6x[2]^10x[3]^2x[4]^6
+ x[1]^2x[2]^14x[3]^2x[4]^6 - x[2]^16x[3]^2x[4]^6 - x[1]^10x[2]^4x[3]^4x[4]^6
+ x[1]^8x[2]^6x[3]^4x[4]^6 + x[1]^6x[2]^8x[3]^4x[4]^6 - x[1]^4x[2]^10x[3]^4x[4]^6
+ x[1]^12x[3]^6x[4]^6 + x[1]^10x[2]^2x[3]^6x[4]^6 + x[1]^8x[2]^4x[3]^6x[4]^6
- x[1]^6x[2]^6x[3]^6x[4]^6 + x[1]^4x[2]^8x[3]^6x[4]^6 + x[1]^2x[2]^10x[3]^6x[4]^6
+ x[2]^12x[3]^6x[4]^6 + x[1]^10x[3]^8x[4]^6 - x[1]^8x[2]^2x[3]^8x[4]^6 + x[1]^6x[2]^4x[3]^8x[4]^6
+ x[1]^4x[2]^6x[3]^8x[4]^6 - x[1]^2x[2]^8x[3]^8x[4]^6 + x[2]^10x[3]^8x[4]^6
+ x[1]^8x[3]^10x[4]^6 + x[1]^6x[2]^2x[3]^10x[4]^6 - x[1]^4x[2]^4x[3]^10x[4]^6
+ x[1]^2x[2]^6x[3]^10x[4]^6 + x[2]^8x[3]^10x[4]^6 + x[1]^6x[3]^12x[4]^6 + x[2]^6x[3]^12x[4]^6
+ x[1]^2x[2]^2x[3]^14x[4]^6 - x[1]^2x[3]^16x[4]^6 - x[2]^2x[3]^16x[4]^6 + x[1]^16x[4]^8
- x[1]^12x[2]^4x[4]^8 + x[1]^10x[2]^6x[4]^8 + x[1]^6x[2]^10x[4]^8 - x[1]^4x[2]^12x[4]^8
+ x[2]^16x[4]^8 - x[1]^12x[2]^2x[3]^2x[4]^8 - x[1]^10x[2]^4x[3]^2x[4]^8 - x[1]^8x[2]^6x[3]^2x[4]^8
- x[1]^6x[2]^8x[3]^2x[4]^8 - x[1]^4x[2]^10x[3]^2x[4]^8 - x[1]^2x[2]^12x[3]^2x[4]^8
- x[1]^12x[3]^4x[4]^8 - x[1]^10x[2]^2x[3]^4x[4]^8 - x[1]^8x[2]^4x[3]^4x[4]^8
+ x[1]^6x[2]^6x[3]^4x[4]^8 - x[1]^4x[2]^8x[3]^4x[4]^8 - x[1]^2x[2]^10x[3]^4x[4]^8
- x[2]^12x[3]^4x[4]^8 + x[1]^10x[3]^6x[4]^8 - x[1]^8x[2]^2x[3]^6x[4]^8 + x[1]^6x[2]^4x[3]^6x[4]^8
+ x[1]^4x[2]^6x[3]^6x[4]^8 - x[1]^2x[2]^8x[3]^6x[4]^8 + x[2]^10x[3]^6x[4]^8
- x[1]^6x[2]^2x[3]^8x[4]^8 - x[1]^4x[2]^4x[3]^8x[4]^8 - x[1]^2x[2]^6x[3]^8x[4]^8
+ x[1]^6x[3]^10x[4]^8 - x[1]^4x[2]^2x[3]^10x[4]^8 - x[1]^2x[2]^4x[3]^10x[4]^8 + x[2]^6x[3]^10x[4]^8
- x[1]^4x[3]^12x[4]^8 - x[1]^2x[2]^2x[3]^12x[4]^8 - x[2]^4x[3]^12x[4]^8 + x[3]^16x[4]^8
+ x[1]^14x[4]^10 - x[1]^12x[2]^2x[4]^10 + x[1]^8x[2]^6x[4]^10 + x[1]^6x[2]^8x[4]^10
- x[1]^2x[2]^12x[4]^10 + x[2]^14x[4]^10 - x[1]^12x[3]^2x[4]^10 - x[1]^10x[2]^2x[3]^2x[4]^10
- x[1]^8x[2]^4x[3]^2x[4]^10 + x[1]^6x[2]^6x[3]^2x[4]^10 - x[1]^4x[2]^8x[3]^2x[4]^10
- x[1]^2x[2]^10x[3]^2x[4]^10 - x[2]^12x[3]^2x[4]^10 - x[1]^8x[2]^2x[3]^4x[4]^10
- x[1]^6x[2]^4x[3]^4x[4]^10 - x[1]^4x[2]^6x[3]^4x[4]^10 - x[1]^2x[2]^8x[3]^4x[4]^10
```

```
+ x[1]^8x[3]^6x[4]^10 + x[1]^6x[2]^2x[3]^6x[4]^10 - x[1]^4x[2]^4x[3]^6x[4]^10
+ x[1]^2x[2]^6x[3]^6x[4]^10 + x[2]^8x[3]^6x[4]^10 + x[1]^6x[3]^8x[4]^10 - x[1]^4x[2]^2x[3]^8x[4]^10
- x[1]^2x[2]^4x[3]^8x[4]^10 + x[2]^6x[3]^8x[4]^10 - x[1]^2x[2]^2x[3]^10x[4]^10
- x[1]^2x[3]^12x[4]^10 - x[2]^2x[3]^12x[4]^10 + x[3]^14x[4]^10 - x[1]^10x[2]^2x[4]^12
- x[1]^8x[2]^4x[4]^12 + x[1]^6x[2]^6x[4]^12 - x[1]^4x[2]^8x[4]^12 - x[1]^2x[2]^10x[4]^12
- x[1]^10x[3]^2x[4]^12 - x[1]^8x[2]^2x[3]^2x[4]^12 - x[1]^2x[2]^8x[3]^2x[4]^12
- x[2]^10x[3]^2x[4]^12 - x[1]^8x[3]^4x[4]^12 - x[1]^4x[2]^4x[3]^4x[4]^12 - x[2]^8x[3]^4x[4]^12
+ x[1]^6x[3]^6x[4]^12 + x[2]^6x[3]^6x[4]^12 - x[1]^4x[3]^8x[4]^12 - x[1]^2x[2]^2x[3]^8x[4]^12
- x[2]^4x[3]^8x[4]^12 - x[1]^2x[3]^10x[4]^12 - x[2]^2x[3]^10x[4]^12 + x[1]^10x[4]^14
+ x[2]^10x[4]^14 + x[1]^6x[2]^2x[3]^2x[4]^14 + x[1]^4x[2]^4x[3]^2x[4]^14
+ x[1]^2x[2]^6x[3]^2x[4]^14 + x[1]^4x[2]^2x[3]^4x[4]^14 + x[1]^2x[2]^4x[3]^4x[4]^14
+ x[1]^2x[2]^2x[3]^6x[4]^14 + x[3]^10x[4]^14 + x[1]^8x[4]^16 - x[1]^6x[2]^2x[4]^16
- x[1]^4x[2]^4x[4]^16 - x[1]^2x[2]^6x[4]^16 + x[2]^8x[4]^16 - x[1]^6x[3]^2x[4]^16
+ x[1]^4x[2]^2x[3]^2x[4]^16 + x[1]^2x[2]^4x[3]^2x[4]^16 - x[2]^6x[3]^2x[4]^16 - x[1]^4x[3]^4x[4]^16
+ x[1]^2x[2]^2x[3]^4x[4]^16 - x[2]^4x[3]^4x[4]^16 - x[1]^2x[3]^6x[4]^16 - x[2]^2x[3]^6x[4]^16
+ x[3]^8x[4]^16 + x[1]^4x[2]^2x[4]^18 + x[1]^2x[2]^4x[4]^18 + x[1]^4x[3]^2x[4]^18
- x[1]^2x[2]^2x[3]^2x[4]^18 + x[2]^4x[3]^2x[4]^18 + x[1]^2x[3]^4x[4]^18 + x[2]^2x[3]^4x[4]^18
+ x[1]^4x[4]^20 + x[1]^2x[2]^2x[4]^20 + x[2]^4x[4]^20 + x[1]^2x[3]^2x[4]^20 + x[2]^2x[3]^2x[4]^20
+ x[3]^4x[4]^20 + x[1]^2x[4]^22 + x[2]^2x[4]^22 + x[3]^2x[4]^22 + x[4]^24
```

Appendix B

Testing the conjecture 4.1

B.1 The d_i polynomials for $n = 3$, $i = 2$ and for small values of q

These polynomials were generated using maple code following the algorithm given in §4.3 with $\xi_0 = x_1^2 + x_2^2 + x_3^2$ and for $q = 3, 5, 7, 9$.

To save space we give the polynomials in the following shorthand. This code was used in the Maple code that was written for the generation of the ϕ_i's and d_i's.

$$[a, b, c] = x^a y^b z^c + x^a y^c z^b + x^b y^a z^c + x^b y^c z^a + x^c y^b z^a + x^c y^a z^b$$

$$[a, a, b] \text{ or } [a, b, a] \text{ or } [b, a, a] = x^a y^a z^b + x^a y^b z^a + x^b y^a z^a$$

$$[a, a, a] = x^a y^a z^a$$

- $q = 3$

$$2[4, 2, 0] + 2[2, 2, 2]$$

- $q = 5$

$$3[20, 0, 0] + 2[18, 2, 0] + [16, 4, 0] + [16, 2, 2] + 4[14, 6, 0] + [12, 8, 0]$$
$$+[12, 6, 2] + [12, 4, 4] + 2[10, 10, 0] + 3[10, 8, 2] + 2[10, 6, 4] + 2[8, 6, 6]$$
$$+[8, 8, 4]$$

- $q = 7$

$$2[42,0,0] + [40,2,0] + 3[38,4,0] + 6[38,2,2] + 6[36,6,0] + 4[36,4,2]$$
$$+2[34,8,0] + 6[32,10,0] + 6[32,8,2] + 6[30,12,0] + 2[30,10,2] + 6[30,8,4]$$
$$+6[30,6,6] + 4[28,14,0] + 2[26,16,0] + 3[26,14,2] + 5[26,8,8] + 6[24,18,0]$$
$$+5[24,16,2] + 4[24,14,4] + 6[24,12,6] + 3[24,10,8] + 5[22,20,0] + 3[22,18,2]$$
$$+3[22,14,6] + [22,12,8] + 5[20,14,8] + 6[18,18,6] + 4[18,16,8] + 2[18,14,10]$$
$$+6[18,12,12] + 5[16,14,12] + 6[14,14,14]$$

- $q = 9$

$$[72,0,0] + [70,2,0] + [68,4,0] + 2[68,2,2] + 2[66,6,0] + 2[64,8,0] + [64,4,4]$$
$$+2[62,10,2] + 2[60,12,0] + 2[60,10,2] + [58,14,0] + 2[58,12,2] + [58,10,4]$$
$$+2[56,16,0] + 2[56,8,8] + 2[54,18,0] + 2[54,16,2] + [54,14,4] + 2[54,12,6]$$
$$+[54,10,8] + [52,18,2] + [52,10,10] + 2[48,24,0] + [48,22,2] + [48,18,6]$$
$$+2[48,16,8] + [48,14,10] + 2[46,24,2] + 2[46,18,8] + 2[46,16,10] + [44,28,0]$$
$$+[44,18,10] + 2[42,30,0] + 2[40,32,0] + [40,30,2] + 2[40,28,4] + 2[40,24,8]$$
$$+[40,22,10] + [40,18,14] + 2[40,16,16] + [38,34,0] + 2[38,32,2] + 2[38,30,4]$$
$$+[38,28,6] + 2[38,24,10] + 2[38,18,16] + [36,36,0] + 2[36,34,2] + 2[36,32,4]$$
$$+[36,28,8] + [36,18,18] + [34,28,10] + 2[32,32,8] + 2[32,28,12] + 2[32,24,16]$$
$$+[32,22,18] + 2[30,30,12] + 2[30,28,14] + 2[30,24,18] + [28,28,16] + 2[24,24,24]$$

B.2 Code for $n = 4, q = 3$ and $i = 3$ and $\xi_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$

```
-- This CoCoA code finds the polynomial Phi(N-1) in the Xi's such that
-- C(N,N-1)+Phi(N-1) is a Qth power where C(N,I) is the Ith Dickson invariant for given I.

N:=4; MEMORY.N:=N; P:=3; MEMORY.P:=P; D:=1; Q:=P^D; MEMORY.Q:=Q; I:=3; MEMORY.I:=I; Nm:=N-1;
Use RR::=Z/(P)[t,x[1..N],s[0..Nm]];RR;

-----------------------------------------------------------------------

-- C calculates Dickson invariant C(N,I)from Dickson matrix DM(N)
-- CF is the list of coefficients of powers of t in the determinant of DM in descending order

Define C(N,I)
    N:=MEMORY.N; Q:=MEMORY.Q;  I:=MEMORY.I; DM:=NewMat(N+1,N+1);
    For A:=1 To N+1 Do For B:=1 To N Do DM[A,B]:=x[B]^(Q^(A-1) EndFor;
    DM[A,N+1]:=t^(Q^(A-1)) EndFor;
    CF:=Coefficients(Det(DM),t); C:=CF[Q^N-Q^I+1]/CF[1];
Return C EndDefine;

DC:=Deg(C(N,I)); MEMORY.DC:=DC; PrintLn("The degree of c(n,i) is ",DC);

-----------------------------------------------------------------------

-- The procedure Xi(I) generates the Xi(j)s from Xi(0):=x[1]^2+....+ x[n]^2

Define Xi(I)
    Q:=MEMORY.Q; N:=MEMORY.N; Xi:=0;
    For A:=1 To N Do Xi:=Xi+x[A]^(Q^I+1) EndFor;
Return Xi EndDefine;
-----------------------------------------------------------------------

-- Exp(A3,A2,A1) generates expressions in the Xi's of degree DC=degof C(N,I)
-- Only Xi's up to Xi(N-1) need be considered as deg(Xi(N))> DC
-- AI is the degree of Xi(I) for I=0,1,2 in Exp(A3,A2,A1)

Define Exp(A3,A2,A1)
    N:=MEMORY.N; Q:=MEMORY.Q;  DC:=MEMORY.DC;
```

```
    A0:=(DC-A3*(Q^3+1)-A2*(Q^2+1)-A1*(Q+1))/2;
    Exp:=Xi(3)^A3*Xi(2)^A2*Xi(1)^A1*Xi(0)^A0;
Return Exp EndDefine;

-----------------------------------------------------------------------

-- NExpr is the number of possible polynomials Exp(A3,A2,A1) that are not themselves Qth powers
-- A3H is the max possible degree of Xi(N-1) for use in the Exp(A3,A2,A1)

A3H:=Div(DC,(Q^(N-1)+1)); NExpr:=0;
For A3:=0 To A3H Do A2H:=Div((DC-A3*(Q^3+1)),(Q+1));
    For A2:=0 To A2H Do A1H:=Div((DC-A3*(Q^3+1)-A2*(Q^2+1)),(Q+1));
        For A1:=0 To A1H Do
            If Mod(A3,Q)<>0 OR Mod(A2,Q)<>0 OR Mod(A1,Q)<>0 Then NExpr:=NExpr+1;
EndIf EndFor EndFor EndFor;
PrintLn("The number of non Qth power expressions is ",NExpr);
MEMORY.NExpr:=NExpr;

-----------------------------------------------------------------------

-- NTerms is the maximum number of terms in the homogeneous polynomials of degree
-- equal to that of C(N,I) that are not Qth powers, that have all even indices
-- and that are distinct (terms with permuted indices are not counted as distinct)

NTerms:=0; For Degx1:=DC To Div(DC,N) Step -2 Do
    DegRem1:=DC-Degx1; Deg1:=Min([DegRem1,Degx1]);
    For Degx2:=Deg1 To Div(DegRem1,N-1) Step -2 Do
        DegRem2:=DC-Degx1-Degx2; Deg2:=Min([DegRem2,Degx2]);
        For Degx3:=Deg2 To Div(DegRem2,N-2) Step -2 Do
            If Mod(Degx1,Q)<>0 Or Mod(Degx2,Q)<>0 Or Mod(Degx3,Q)<>0 Then NTerms:=NTerms+1;
EndIf EndFor EndFor EndFor;
PrintLn("The number of 'distinct' non Qth power terms is ",NTerms);
MEMORY.NTerms:=NTerms;

-----------------------------------------------------------------------

-- ExpCoeffs extracts the coefficients of terms in a given polynomial that are not
-- Qth powers but that have constituent indices even.
```

```
-- Also to reduce size of the calculation the  'symmetrical' coefficients have been removed

Define ExpCoeffs(Ply)
    N:=MEMORY.N; Q:=MEMORY.Q; P:=MEMORY.P; Deg:=Deg(Ply); NTerms:=MEMORY.NTerms;
    Count:=1; CoeffList:=NewList(NTerms);
    For Degx1:=Deg To Div(Deg,N) Step -2 Do
        DegRem1:=Deg-Degx1; Deg1:=Min([DegRem1,Degx1]);
        For Degx2:=Deg1 To Div(DegRem1,N-1) Step -2 Do
            DegRem2:=Deg-Degx1-Degx2; Deg2:=Min([DegRem2,Degx2]);
            For Degx3:=Deg2 To Div(DegRem2,N-2) Step -2 Do
                If Mod(Degx1,Q)<>0 Or Mod(Degx2,Q)<>0 Or Mod(Degx3,Q)<>0 Then
                    Degx4:=Deg-Degx1-Degx2-Degx3;
                    CoeffList[Count]:=Mod((CoeffOfTerm(x[1]^Degx1*x[2]^Degx2*
                    x[3]^Degx3*x[4]^Degx4,Ply)*(1%P)),P); Count:=Count+1;
    EndIf EndFor EndFor EndFor;
Return CoeffList EndDefine;

-------------------------------------------------------------------------

-- CoeffMat is a matrix whose rows contain the "usable" coefficients of the Exp(A3,A2,A1)
-- polynomials in the Xi(J)s and of C(N,I)

CoeffMat:=NewMat(NExpr+1,NTerms);
A3H:=Div(DC,(Q^(N-1)+1)); Count1:=1; For A3:=0 To A3H Do A2H:=Div((DC-A3*(Q^3+1)),(Q+1));
    For A2:=0 To A2H Do A1H:=Div((DC-A3*(Q^3+1)-A2*(Q^2+1)),(Q+1));
        For A1:=0 To A1H Do If Mod(A3,Q)<>0 OR Mod(A2,Q)<>0 OR Mod(A1,Q)<>0 Then
            CoeffMat[Count1]:=ExpCoeffs(Exp(A3,A2,A1)); Count1:=Count1+1;
EndIf EndFor EndFor EndFor;
CoeffMat[NExpr+1]:=ExpCoeffs(C(N,I));

---------------------------------------------------------------------

-- The following procedures reduces the transpose of the coefficient matrix to reduced
-- row echelon form leaving the last column of the transposed matrix as the solution vector.
-- RowDiv returns the matrix M with Ath row scaled to give M[A,A]=1 if M[A,A]<>0
-- Needs the XInv procedure to find multiplicative inverse of M[A,A]

Define XInv(I)
```

```
    For A:=1 To MEMORY.Q-1 Do B:=I*A;
        If Mod(B,MEMORY.P)=1 Then XInv:=A
    EndIf EndFor;
Return XInv EndDefine;

Define RowDiv(M,A) Rows:=Len(M); Cols:=Len(M[1]); Pivot:=M[A,A];
    If Pivot<>0 Then PDiv:=XInv(Pivot);
        For B:=1 To Cols Do M[A,B]:=Mod(M[A,B]*PDiv,MEMORY.P) EndFor;
    EndIf;
Return M EndDefine;

-- For each row, check whether M[A,A]<>0.
-- If so do Row Div and subtract M[B,A]*Row A from Row B row.
-- If M[A,A]=0 then find a M[B,A]<>0 if one exists for B>A and exchange rows then do above

Define ColClear(M,A) Rows:=Len(M); Cols:=Len(M[1]);
    If M[A,A]=0 Then Temp:=M[A];
        For B:=A+1 To Rows Do
            If M[B,A]<>0 Then
                M[A]:=M[B]; M[B]:=Temp; Break
    EndIf EndFor EndIf;
    If M[A,A]<>0 Then M:=RowDiv(M,A);
        For B:=1 To Rows Do If B<>A Then Scal:=M[B,A];
            For B1:=1 To Cols Do M[B,B1]:=Mod(M[B,B1]-M[A,B1]*Scal,MEMORY.P);
    EndFor EndIf EndFor EndIf;
Return M; EndDefine;

-- RowRed reduces an augmented matrix to reduced row echelon form

Define RowRed(M) Rows:=Len(M); Cols:=Len(M[1]); Reps:=Min(Cols-1,Rows);
    For A:=1 To Reps Do --PrintLn(A); M:=ColClear(M,A) EndFor;
Return M; EndDefine;

-------------------------------------------------------------------------

--The procedures are now implemented to calculate the Phi(i) polynomials
--Sol is the list of coefficients of possible expressions in the Xi's
```

```
SM:=RowRed(Transposed(CoeffMat));
Cols:=Len(SM[1]); Cols1:=Cols-1;
SMT:=Transposed(SM); Sol:=Submat(SMT,[Cols],1..Cols1);
PrintLn("Solutions for n=",N,"and q=",Q," are ",Sol);

-- Generation of the polynomial Phi(i) in the Xi's from the solution matrix Sol found above
-- XiDegMat is the matrix containing in each column the degrees of the xi's in each possible
-- expression in the xi's of degree equal to that of C(N,I);
Define XiDegMat(N,Q) N:=MEMORY.N; NExpr:=MEMORY.NExpr;
    DC:=Q^N-Q^(N-1); A3H:=Div(DC,(Q^(N-1)+1));
    XiDegMat:=NewMat(N,NExpr);Count:=1;
    For A3:=0 To A3H Do A2H:=Div((DC-A3*(Q^3+1)),(Q+1));
        For A2:=0 To A2H Do A1H:=Div((DC-A3*(Q^3+1)-A2*(Q^2+1)),(Q+1));
            For A1:=0 To A1H Do If Mod(A3,Q)<>0 OR Mod(A2,Q)<>0 OR Mod(A1,Q)<>0 Then
                A0:=(DC-A3*(Q^3+1)-A2*(Q^2+1)-A1*(Q+1))/2;
                XiDegMat[1,Count]:=A3; XiDegMat[2,Count]:=A2;
                XiDegMat[3,Count]:=A1;  XiDegMat[4,Count]:=A0; Count:=Count+1;
    EndIf EndFor EndFor EndFor;
Return XiDegMat EndDefine;
PrintLn("The matrix of degrees of the Xi's in the possible terms of Phi(i) is ",XiDegMat(N,Q));

-----------------------------------------------------------------

-- The Phi procedure produces the polynomial Phi in the xi's from the Sol list and XiDegMat matrix
Define Phi(Sol,M) N:=MEMORY.N; Phi:=0;
    For A:=1 To Len(Sol[1])
        Do Phi:=Phi+Sol[1,A]*(s[3]^(M[1,A])*s[2]^(M[2,A])*s[1]^(M[3,A])*s[0]^(M[4,A]));
    EndFor;
Return Phi EndDefine;
-- Phii is the polynomial Phi
Phii:=Phi(Sol,XiDegMat(N,Q)); PrintLn("When q:=",Q," Phi(N-1) is ",Phii);

-------------------------------------------------------------------

Diq is now calculated by definition given in the Conjecture
Diq:=C(N,I)-Subst(Phii,[[s[0],Xi(0)],[s[1],Xi(1)],[s[2],Xi(2)],[s[3],Xi(3)]]);
PrintLn("d_i^q=",Di);
```

B.3 Output for n=4

```
Z/(3)[t,x[1..4],s[0..3]]
--------------------------------

The degree of c(n,i) is 54
--------------------------------

The number of non Qth power expressions is 54
--------------------------------

The number of 'distinct' non Qth power terms is 207
--------------------------------

Solutions for n=4 and q=3 are Mat([
  [0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
   0, 0, 0, 0, 0, 2, 0, 2, 2, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0]])
--------------------------------
When q:=3 Phi(3) is -s[0]s[1]^13 + s[0]^4s[1]^9s[2] +s[0]^10s[1]s[2]^3
- s[0]^13s[3] - s[1]^11s[2] + s[0]^9s[1]^2s[3] -s[0]s[1]^3s[2]^4 + s[0]s[1]^6s[3]
- s[1]s[2]^5 + s[1]^4s[2]s[3] +s[0]^3s[2]^2s[3]
--------------------------------

d_i^q=x[1]^54 - x[1]^48x[2]^6 - x[1]^42x[2]^12 - x[1]^36x[2]^18 +x[1]^30x[2]^24 + x[1]^24x[2]^30
- x[1]^18x[2]^36 - x[1]^12x[2]^42 - x[1]^6x[2]^48 + x[2]^54 - x[1]^48x[3]^6 - x[1]^36x[2]^12x[3]^6
+ x[1]^30x[2]^18x[3]^6 + x[1]^18x[2]^30x[3]^6 - x[1]^12x[2]^36x[3]^6 - x[2]^48x[3]^6
- x[1]^42x[3]^12 - x[1]^36x[2]^6x[3]^12 + x[1]^30x[2]^12x[3]^12 + x[1]^12x[2]^30x[3]^12
- x[1]^6x[2]^36x[3]^12 - x[2]^42x[3]^12 - x[1]^36x[3]^18 + x[1]^30x[2]^6x[3]^18
- x[1]^18x[2]^18x[3]^18 + x[1]^6x[2]^30x[3]^18 - x[2]^36x[3]^18 + x[1]^30x[3]^24
+ x[2]^30x[3]^24 + x[1]^24x[3]^30 + x[1]^18x[2]^6x[3]^30 + x[1]^12x[2]^12x[3]^30
+ x[1]^6x[2]^18x[3]^30 + x[2]^24x[3]^30 - x[1]^18x[3]^36 - x[1]^12x[2]^6x[3]^36
- x[1]^6x[2]^12x[3]^36 - x[2]^18x[3]^36 - x[1]^12x[3]^42 - x[2]^12x[3]^42 - x[1]^6x[3]^48
- x[2]^6x[3]^48 + x[3]^54 - x[1]^48x[4]^6 - x[1]^36x[2]^12x[4]^6 + x[1]^30x[2]^18x[4]^6
+ x[1]^18x[2]^30x[4]^6 - x[1]^12x[2]^36x[4]^6- x[2]^48x[4]^6 - x[1]^36x[2]^6x[3]^6x[4]^6
+ x[1]^30x[2]^12x[3]^6x[4]^6 + x[1]^12x[2]^30x[3]^6x[4]^6
- x[1]^6x[2]^36x[3]^6x[4]^6 - x[1]^36x[3]^12x[4]^6 + x[1]^30x[2]^6x[3]^12x[4]^6
- x[1]^18x[2]^18x[3]^12x[4]^6 + x[1]^6x[2]^30x[3]^12x[4]^6 - x[2]^36x[3]^12x[4]^6
+ x[1]^30x[3]^18x[4]^6 - x[1]^18x[2]^12x[3]^18x[4]^6 - x[1]^12x[2]^18x[3]^18x[4]^6
```

```
+ x[2]^30x[3]^18x[4]^6 + x[1]^18x[3]^30x[4]^6 + x[1]^12x[2]^6x[3]^30x[4]^6
+ x[1]^6x[2]^12x[3]^30x[4]^6 + x[2]^18x[3]^30x[4]^6 - x[1]^12x[3]^36x[4]^6
- x[1]^6x[2]^6x[3]^36x[4]^6 - x[2]^12x[3]^36x[4]^6 - x[3]^48x[4]^6 - x[1]^42x[4]^12
- x[1]^36x[2]^6x[4]^12 + x[1]^30x[2]^12x[4]^12 + x[1]^12x[2]^30x[4]^12 - x[1]^6x[2]^36x[4]^12
- x[2]^42x[4]^12 - x[1]^36x[3]^6x[4]^12 + x[1]^30x[2]^6x[3]^6x[4]^12
- x[1]^18x[2]^18x[3]^6x[4]^12 + x[1]^6x[2]^30x[3]^6x[4]^12 - x[2]^36x[3]^6x[4]^12
+ x[1]^30x[3]^12x[4]^12 - x[1]^18x[2]^12x[3]^12x[4]^12 - x[1]^12x[2]^18x[3]^12x[4]^12
+ x[2]^30x[3]^12x[4]^12 - x[1]^18x[2]^6x[3]^18x[4]^12 - x[1]^12x[2]^12x[3]^18x[4]^12
- x[1]^6x[2]^18x[3]^18x[4]^12 + x[1]^12x[3]^30x[4]^12 + x[1]^6x[2]^6x[3]^30x[4]^12
+ x[2]^12x[3]^30x[4]^12 - x[1]^6x[3]^36x[4]^12 - x[2]^6x[3]^36x[4]^12 - x[3]^42x[4]^12
- x[1]^36x[4]^18 + x[1]^30x[2]^6x[4]^18 - x[1]^18x[2]^18x[4]^18 + x[1]^6x[2]^30x[4]^18
- x[2]^36x[4]^18 + x[1]^30x[3]^6x[4]^18 - x[1]^18x[2]^12x[3]^6x[4]^18 - x[1]^12x[2]^18x[3]^6x[4]^18
+ x[2]^30x[3]^6x[4]^18 - x[1]^18x[2]^6x[3]^12x[4]^18 - x[1]^12x[2]^12x[3]^12x[4]^18
- x[1]^6x[2]^18x[3]^12x[4]^18 - x[1]^18x[3]^18x[4]^18 - x[1]^12x[2]^6x[3]^18x[4]^18
- x[1]^6x[2]^12x[3]^18x[4]^18 - x[2]^18x[3]^18x[4]^18 + x[1]^6x[3]^30x[4]^18 + x[2]^6x[3]^30x[4]^18
- x[3]^36x[4]^18 + x[1]^30x[4]^24 + x[2]^30x[4]^24 + x[3]^30x[4]^24 + x[1]^24x[4]^30
+ x[1]^18x[2]^6x[4]^30 + x[1]^12x[2]^12x[4]^30 + x[1]^6x[2]^18x[4]^30 + x[2]^24x[4]^30
+ x[1]^18x[3]^6x[4]^30 + x[1]^12x[2]^6x[3]^6x[4]^30 + x[1]^6x[2]^12x[3]^6x[4]^30
+ x[2]^18x[3]^6x[4]^30 + x[1]^12x[3]^12x[4]^30 + x[1]^6x[2]^6x[3]^12x[4]^30 + x[2]^12x[3]^12x[4]^30
+ x[1]^6x[3]^18x[4]^30 + x[2]^6x[3]^18x[4]^30 + x[3]^24x[4]^30 - x[1]^18x[4]^36
- x[1]^12x[2]^6x[4]^36 - x[1]^6x[2]^12x[4]^36 - x[2]^18x[4]^36 - x[1]^12x[3]^6x[4]^36
- x[1]^6x[2]^6x[3]^6x[4]^36 - x[2]^12x[3]^6x[4]^36 - x[1]^6x[3]^12x[4]^36 - x[2]^6x[3]^12x[4]^36
- x[3]^18x[4]^36 - x[1]^12x[4]^42 - x[2]^12x[4]^42 - x[3]^12x[4]^42 - x[1]^6x[4]^48 - x[2]^6x[4]^48
- x[3]^6x[4]^48 + x[4]^54
--------------------------------
```

B.4 Code to find the d_i's explicitly when $n = 4$

.

```
-- This CoCoA code finds the polynomials D4i in the x's as the qth root
-- of C(N,N-1)+Phi(N-1) where C(N,I) is the Ith Dickson invariant.
N:=4; MEMORY.N:=N; P:=3; MEMORY.P:=P;  Q:=P; MEMORY.Q:=Q; Nm:=N-1;
Use RR::=Z/(P)[t,x[1..N],s[0..Nm]];RR;
-----------------------------------------------------------------------

-- C calculates Dickson invariant C(N,I)from Dickson matrix DM(N)
-- CF is the list of coefficients of powers of t in the determinant of DM in descending order

Define C(N,I) Q:=MEMORY.Q; DM:=NewMat(N+1,N+1);
    For A:=1 To N+1 Do For B:=1 To N Do  DM[A,B]:=x[B]^(Q^(A-1))
    EndFor; DM[A,N+1]:=t^(Q^(A-1)) EndFor;
    CF:=Coefficients(Det(DM),t); C:=CF[Q^N-Q^I+1]/CF[1];
Return C EndDefine;
-----------------------------------------------------------------------
-- The procedure Xi(I) generates the Xi(j)s from  Xi(0):=x[1]^2+....+ x[n]^2

Define Xi(J) Q:=MEMORY.Q; N:=MEMORY.N; Xi:=0;
    For A:=1 To N Do Xi:=Xi+x[A]^(Q^J+1) EndFor;
Return Xi EndDefine;

-----------------------------------------------------------------------

-- NTerms is the maximum number of terms in the homogeneous polynomials
-- of degree equal to that of C(N,I) that are not Qth powers,
-- that have all even indices and that are distinct
-- (terms with permuted indices are not counted as distinct)
Define NTerms(Ply) DC:=Deg(Ply); NTerms:=0;
    For Degx1:=DC To 0 Step -2 Do For Degx2:=DC-Degx1 To 0 Step -2 Do
         For Degx3:=DC-Degx1-Degx2 To 0 Step -2 Do NTerms:=NTerms+1;
    EndFor; EndFor; EndFor;
    PrintLn("The number of terms is ",NTerms);
Return NTerms EndDefine;
-----------------------------------------------------------------------
```

```
-- DEGS is the matrix containing the degrees of the indeterminates in all
-- possible terms of degree equal to that of the input polynomial
Define DEGS(Ply) N:=MEMORY.N; DC:=Deg(Ply); NTerms:=NTerms(Ply);
    DEGS:=NewMat(NTerms,N); DEGSCount:=1;
    For Degx1:=DC To 0 Step -2 Do For Degx2:=DC-Degx1 To 0 Step -2 Do
        For Degx3:=DC-Degx1-Degx2 To 0 Step -2 Do Degx4:=DC-Degx1-Degx2-Degx3;
            DEGS[DEGSCount,1]:=Degx1; DEGS[DEGSCount,2]:=Degx2;
            DEGS[DEGSCount,3]:=Degx3; DEGS[DEGSCount,4]:=Degx4;
            DEGSCount:=DEGSCount+1;
    EndFor; EndFor; EndFor;
Return DEGS; EndDefine;
-----------------------------------------------------------------------

-- ExpCoeffs extracts the coefficients of terms in a given polynomial that are not
-- Qth powers but that have constituent indices even.
-- To reduce size of the calculation the 'symmetrical' coefficients have been removed

Define ExpCoeffs(Ply) N:=MEMORY.N; Q:=MEMORY.Q; P:=MEMORY.P; Deg:=Deg(Ply);
    NTerms:=NTerms(Ply); Count:=1; CoeffList:=NewList(NTerms);
    For Degx1:=Deg To 0 Step -2 Do For Degx2:=Deg-Degx1 To 0 Step -2 Do
        For Degx3:=Deg-Degx1-Degx2 To 0 Step -2 Do Degx4:=Deg-Degx1-Degx2-Degx3;
            CoeffList[Count]:=Mod((CoeffOfTerm(x[1]^Degx1*x[2]^Degx2*
            x[3]^Degx3*x[4]^Degx4,Ply)*(1%P)),P); Count:=Count+1;
    EndFor; EndFor; EndFor;
Return CoeffList EndDefine;
-----------------------------------------------------------------------

--Phi4 is the list of Ph41,Phi42, Phi43 calculated in the previous code

Phi4:=[s[0]^37s[1] - s[0]^28s[1]^3s[2] - s[0]^27s[1]s[2]^2 - s[0]s[1]^19
+ s[0]s[1]^9s[2]^4 + s[0]s[1]^12s[3] - s[0]^10s[2]^3s[3] - s[1]^10s[2]s[3]
- s[0]^9s[1]s[3]^2 + s[2]^5s[3] + s[1]^3s[2]s[3]^2, -s[0]^28s[1]^4 + s[0]^31s[2]
- s[0]^27s[1]^2s[2] + s[0]s[1]^10s[2]^3 - s[0]^4s[1]^9s[3] + s[1]^11s[3]
- s[0]s[2]^7 + s[0]s[1]^3s[2]^3s[3] - s[1]s[2]^4s[3] + s[1]^4s[3]^2
- s[0]^3s[2]s[3]^2, s[0]s[1]^13 - s[0]^4s[1]^9s[2] - s[0]^10s[1]s[2]^3
+ s[0]^13s[3] + s[1]^11s[2] - s[0]^9s[1]^2s[3] + s[0]s[1]^3s[2]^4
- s[0]s[1]^6s[3] + s[1]s[2]^5 - s[1]^4s[2]s[3] - s[0]^3s[2]^2s[3]];
-----------------------------------------------------------------------
```

```
-- SubList is the list of the substitutions in the map to express the
-- polynomials in the x[i]'s
-- D4iq is the list of the D4i polynomials for I:=1 To 3
SubList:=[s[1],Xi(1)],[s[2],Xi(2)],[s[3],Xi(3)]]
D4iq:=[C(N,I)+Subst(Phi4[I],SubList)|I In 1..3];

-----------------------------------------------------------------------

--D4iqCoeffs is the list of the coefficients of the D4iq
--for I:= 1 To 3
D4iqCoeffs:=[ExpCoeffs(D4iq[I])|I In 1..3];

-----------------------------------------------------------------------

--D4i is the list of D4i for I=1 ..3, the qth roots of the D4iq
D4i:=NewList(3);
For I:=1 To 3 Do D4iqCo:=D4iqCoeffs[I];
    DEGS:=DEGS(C(N,I)); NTerms:=NTerms(C(N,I)); D4i[I]:=0;
    For J:=1 To NTerms Do If D4iqCo[J]<>0 Then Term:=1;
        For K:=1 To N Do DR:=(DEGS[J,K])/Q; Term:=Term*x[K]^DR EndFor;
        D4i[I]:=D4i[I]+D4iqCo[J]*Term;
EndIf; EndFor; EndFor;

-----------------------------------------------------------------------

--We check that we have the qth roots and that the D4i fit the definitions of the conjecture
For I:= 1 To 3 Do PrintLn; PrintLn 'N=',N,' Q=',Q,' I=',I;
    If D4i[I]^Q=D4iq[I] Then PrintLn 'D4',I,'=',D4i[I] Else PrintLn 'FALSE' EndIf;
EndFor;
For I:= 1 To 3 Do D4i[I]^Q=Subst(C(N,I)+Phi4[I],SubList) EndFor;
```

B.5 The d_i polynomials when $n = 4$

The explicit expressions for the invariants $d_i = d_i(x_1, x_2, x_3, x_4)$ for $i = 1, 2, 3$ that are output from the code in the previous section are given here as D41, D42 and D43 respectively.

```
N=4 Q=3 I=1
D41=-x[1]^26 + x[1]^22x[2]^4 - x[1]^20x[2]^6 - x[1]^18x[2]^8 + x[1]^16x[2]^10 - x[1]^14x[2]^12
- x[1]^12x[2]^14 + x[1]^10x[2]^16 - x[1]^8x[2]^18 - x[1]^6x[2]^20 + x[1]^4x[2]^22 - x[2]^26
+ x[1]^22x[3]^4 + x[2]^22x[3]^4 - x[1]^20x[3]^6 - x[2]^20x[3]^6 - x[1]^18x[3]^8 - x[2]^18x[3]^8
+ x[1]^16x[3]^10 + x[2]^16x[3]^10 - x[1]^14x[3]^12 - x[2]^14x[3]^12 - x[1]^12x[3]^14
- x[2]^12x[3]^14 + x[1]^10x[3]^16 + x[2]^10x[3]^16 - x[1]^8x[3]^18 - x[2]^8x[3]^18
- x[1]^6x[3]^20 - x[2]^6x[3]^20 + x[1]^4x[3]^22 + x[2]^4x[3]^22 - x[3]^26
- x[1]^18x[2]^4x[3]^2x[4]^2 + x[1]^12x[2]^10x[3]^2x[4]^2 + x[1]^10x[2]^12x[3]^2x[4]^2
- x[1]^4x[2]^18x[3]^2x[4]^2 - x[1]^18x[2]^2x[3]^4x[4]^2 - x[1]^10x[2]^10x[3]^4x[4]^2
- x[1]^2x[2]^18x[3]^4x[4]^2 - x[1]^12x[2]^6x[3]^6x[4]^2 - x[1]^6x[2]^12x[3]^6x[4]^2
+ x[1]^12x[2]^2x[3]^10x[4]^2 - x[1]^10x[2]^4x[3]^10x[4]^2 - x[1]^4x[2]^10x[3]^10x[4]^2
+ x[1]^2x[2]^12x[3]^10x[4]^2 + x[1]^10x[2]^2x[3]^12x[4]^2 - x[1]^6x[2]^6x[3]^12x[4]^2
+ x[1]^2x[2]^10x[3]^12x[4]^2 - x[1]^4x[2]^2x[3]^18x[4]^2 - x[1]^2x[2]^4x[3]^18x[4]^2
+ x[1]^22x[4]^4 + x[2]^22x[4]^4 - x[1]^18x[2]^2x[3]^2x[4]^4 - x[1]^10x[2]^10x[3]^2x[4]^4
- x[1]^2x[2]^18x[3]^2x[4]^4 - x[1]^12x[2]^6x[3]^4x[4]^4 - x[1]^6x[2]^12x[3]^4x[4]^4
- x[1]^12x[2]^4x[3]^6x[4]^4 + x[1]^10x[2]^6x[3]^6x[4]^4 + x[1]^6x[2]^10x[3]^6x[4]^4
- x[1]^4x[2]^12x[3]^6x[4]^4 - x[1]^10x[2]^2x[3]^10x[4]^4 + x[1]^6x[2]^6x[3]^10x[4]^4
- x[1]^2x[2]^10x[3]^10x[4]^4 - x[1]^6x[2]^4x[3]^12x[4]^4 - x[1]^4x[2]^6x[3]^12x[4]^4
- x[1]^2x[2]^2x[3]^18x[4]^4 + x[3]^22x[4]^4 - x[1]^20x[4]^6 - x[2]^20x[4]^6
- x[1]^12x[2]^6x[3]^2x[4]^6 - x[1]^6x[2]^12x[3]^2x[4]^6 - x[1]^12x[2]^4x[3]^4x[4]^6
+ x[1]^10x[2]^6x[3]^4x[4]^6 + x[1]^6x[2]^10x[3]^4x[4]^6 - x[1]^4x[2]^12x[3]^4x[4]^6
- x[1]^12x[2]^2x[3]^6x[4]^6 + x[1]^10x[2]^4x[3]^6x[4]^6 + x[1]^4x[2]^10x[3]^6x[4]^6
- x[1]^2x[2]^12x[3]^6x[4]^6 + x[1]^6x[2]^4x[3]^10x[4]^6 + x[1]^4x[2]^6x[3]^10x[4]^6
- x[1]^6x[2]^2x[3]^12x[4]^6 - x[1]^4x[2]^4x[3]^12x[4]^6 - x[1]^2x[2]^6x[3]^12x[4]^6
- x[3]^20x[4]^6 - x[1]^18x[4]^8 - x[2]^18x[4]^8 - x[3]^18x[4]^8 + x[1]^16x[4]^10
+ x[2]^16x[4]^10 + x[1]^12x[2]^2x[3]^2x[4]^10 - x[1]^10x[2]^4x[3]^2x[4]^10
- x[1]^4x[2]^10x[3]^2x[4]^10 + x[1]^2x[2]^12x[3]^2x[4]^10 - x[1]^10x[2]^2x[3]^4x[4]^10
+ x[1]^6x[2]^6x[3]^4x[4]^10 - x[1]^2x[2]^10x[3]^4x[4]^10 + x[1]^6x[2]^4x[3]^6x[4]^10
+ x[1]^4x[2]^6x[3]^6x[4]^10 - x[1]^4x[2]^2x[3]^10x[4]^10 - x[1]^2x[2]^4x[3]^10x[4]^10
+ x[1]^2x[2]^2x[3]^12x[4]^10 + x[3]^16x[4]^10 - x[1]^14x[4]^12 - x[2]^14x[4]^12
+ x[1]^10x[2]^2x[3]^2x[4]^12 - x[1]^6x[2]^6x[3]^2x[4]^12 + x[1]^2x[2]^10x[3]^2x[4]^12
- x[1]^6x[2]^4x[3]^4x[4]^12 - x[1]^4x[2]^6x[3]^4x[4]^12 - x[1]^6x[2]^2x[3]^6x[4]^12
- x[1]^4x[2]^4x[3]^6x[4]^12 - x[1]^2x[2]^6x[3]^6x[4]^12 + x[1]^2x[2]^2x[3]^10x[4]^12
- x[3]^14x[4]^12 - x[1]^12x[4]^14 - x[2]^12x[4]^14 - x[3]^12x[4]^14 + x[1]^10x[4]^16
```

```
+ x[2]^10x[4]^16 + x[3]^10x[4]^16 - x[1]^8x[4]^18- x[2]^8x[4]^18 - x[1]^4x[2]^2x[3]^2x[4]^18
- x[1]^2x[2]^4x[3]^2x[4]^18 - x[1]^2x[2]^2x[3]^4x[4]^18 - x[3]^8x[4]^18 - x[1]^6x[4]^20
- x[2]^6x[4]^20 - x[3]^6x[4]^20 + x[1]^4x[4]^22 + x[2]^4x[4]^22 + x[3]^4x[4]^22 - x[4]^26

N=4 Q=3 I=2
D42=-x[1]^24 - x[1]^22x[2]^2 + x[1]^20x[2]^4 - x[1]^14x[2]^10 - x[1]^10x[2]^14 + x[1]^4x[2]^20
- x[1]^2x[2]^22 - x[2]^24 - x[1]^22x[3]^2 + x[1]^18x[2]^4x[3]^2 - x[1]^12x[2]^10x[3]^2
- x[1]^10x[2]^12x[3]^2 + x[1]^4x[2]^18x[3]^2 - x[2]^22x[3]^2 + x[1]^20x[3]^4
+ x[1]^18x[2]^2x[3]^4 + x[1]^10x[2]^10x[3]^4 + x[1]^2x[2]^18x[3]^4 + x[2]^20x[3]^4
+ x[1]^12x[2]^6x[3]^6 + x[1]^6x[2]^12x[3]^6 - x[1]^14x[3]^10 - x[1]^12x[2]^2x[3]^10
+ x[1]^10x[2]^4x[3]^10 + x[1]^4x[2]^10x[3]^10 - x[1]^2x[2]^12x[3]^10 - x[2]^14x[3]^10
- x[1]^10x[2]^2x[3]^12 + x[1]^6x[2]^6x[3]^12 - x[1]^2x[2]^10x[3]^12 - x[1]^10x[3]^14
- x[2]^10x[3]^14 + x[1]^4x[2]^2x[3]^18 + x[1]^2x[2]^4x[3]^18 + x[1]^4x[3]^20 + x[2]^4x[3]^20
- x[1]^2x[3]^22 - x[2]^2x[3]^22 - x[3]^24 - x[1]^22x[4]^2 + x[1]^18x[2]^4x[4]^2
- x[1]^12x[2]^10x[4]^2 - x[1]^10x[2]^12x[4]^2 + x[1]^4x[2]^18x[4]^2 - x[2]^22x[4]^2
+ x[1]^18x[2]^2x[3]^2x[4]^2 + x[1]^10x[2]^10x[3]^2x[4]^2 + x[1]^2x[2]^18x[3]^2x[4]^2
+ x[1]^18x[3]^4x[4]^2 + x[1]^12x[2]^6x[3]^4x[4]^2 + x[1]^6x[2]^12x[3]^4x[4]^2
+ x[2]^18x[3]^4x[4]^2 + x[1]^12x[2]^4x[3]^6x[4]^2 - x[1]^10x[2]^6x[3]^6x[4]^2
- x[1]^6x[2]^10x[3]^6x[4]^2 + x[1]^4x[2]^12x[3]^6x[4]^2 - x[1]^12x[3]^10x[4]^2
+ x[1]^10x[2]^2x[3]^10x[4]^2 - x[1]^6x[2]^6x[3]^10x[4]^2 + x[1]^2x[2]^10x[3]^10x[4]^2
- x[2]^12x[3]^10x[4]^2 - x[1]^10x[3]^12x[4]^2 + x[1]^6x[2]^4x[3]^12x[4]^2
+ x[1]^4x[2]^6x[3]^12x[4]^2 - x[2]^10x[3]^12x[4]^2 + x[1]^4x[3]^18x[4]^2
+ x[1]^2x[2]^2x[3]^18x[4]^2 + x[2]^4x[3]^18x[4]^2 - x[3]^22x[4]^2 + x[1]^20x[4]^4
+ x[1]^18x[2]^2x[4]^4 + x[1]^10x[2]^10x[4]^4 + x[1]^2x[2]^18x[4]^4 + x[2]^20x[4]^4
+ x[1]^18x[3]^2x[4]^4 + x[1]^12x[2]^6x[3]^2x[4]^4 + x[1]^6x[2]^12x[3]^2x[4]^4
+ x[2]^18x[3]^2x[4]^4 + x[1]^12x[2]^4x[3]^4x[4]^4 - x[1]^10x[2]^6x[3]^4x[4]^4
- x[1]^6x[2]^10x[3]^4x[4]^4 + x[1]^4x[2]^12x[3]^4x[4]^4 + x[1]^12x[2]^2x[3]^6x[4]^4
- x[1]^10x[2]^4x[3]^6x[4]^4 - x[1]^4x[2]^10x[3]^6x[4]^4 + x[1]^2x[2]^12x[3]^6x[4]^4
+ x[1]^10x[3]^10x[4]^4 - x[1]^6x[2]^4x[3]^10x[4]^4 - x[1]^4x[2]^6x[3]^10x[4]^4
+ x[2]^10x[3]^10x[4]^4 + x[1]^6x[2]^2x[3]^12x[4]^4 + x[1]^4x[2]^4x[3]^12x[4]^4
+ x[1]^2x[2]^6x[3]^12x[4]^4 + x[1]^2x[3]^18x[4]^4 + x[2]^2x[3]^18x[4]^4 + x[3]^20x[4]^4
+ x[1]^12x[2]^6x[4]^6 + x[1]^6x[2]^12x[4]^6 + x[1]^12x[2]^4x[3]^2x[4]^6
- x[1]^10x[2]^6x[3]^2x[4]^6 - x[1]^6x[2]^10x[3]^2x[4]^6 + x[1]^4x[2]^12x[3]^2x[4]^6
+ x[1]^12x[2]^2x[3]^4x[4]^6 - x[1]^10x[2]^4x[3]^4x[4]^6 - x[1]^4x[2]^10x[3]^4x[4]^6
+ x[1]^2x[2]^12x[3]^4x[4]^6 + x[1]^12x[3]^6x[4]^6 - x[1]^10x[2]^2x[3]^6x[4]^6
+ x[1]^6x[2]^6x[3]^6x[4]^6 - x[1]^2x[2]^10x[3]^6x[4]^6 + x[2]^12x[3]^6x[4]^6
- x[1]^6x[2]^2x[3]^10x[4]^6 - x[1]^4x[2]^4x[3]^10x[4]^6 - x[1]^2x[2]^6x[3]^10x[4]^6
+ x[1]^6x[3]^12x[4]^6 + x[1]^4x[2]^2x[3]^12x[4]^6 + x[1]^2x[2]^4x[3]^12x[4]^6
```

```
+ x[2]^6x[3]^12x[4]^6 - x[1]^14x[4]^10 - x[1]^12x[2]^2x[4]^10 + x[1]^10x[2]^4x[4]^10
+ x[1]^4x[2]^10x[4]^10 - x[1]^2x[2]^12x[4]^10 - x[2]^14x[4]^10 - x[1]^12x[3]^2x[4]^10
+ x[1]^10x[2]^2x[3]^2x[4]^10 - x[1]^6x[2]^6x[3]^2x[4]^10 + x[1]^2x[2]^10x[3]^2x[4]^10
- x[2]^12x[3]^2x[4]^10 + x[1]^10x[3]^4x[4]^10 - x[1]^6x[2]^4x[3]^4x[4]^10
- x[1]^4x[2]^6x[3]^4x[4]^10 + x[2]^10x[3]^4x[4]^10 - x[1]^6x[2]^2x[3]^6x[4]^10
- x[1]^4x[2]^4x[3]^6x[4]^10 - x[1]^2x[2]^6x[3]^6x[4]^10 + x[1]^4x[3]^10x[4]^10
+ x[1]^2x[2]^2x[3]^10x[4]^10 + x[2]^4x[3]^10x[4]^10 - x[1]^2x[3]^12x[4]^10
- x[2]^2x[3]^12x[4]^10 - x[3]^14x[4]^10 - x[1]^10x[2]^2x[4]^12 + x[1]^6x[2]^6x[4]^12
- x[1]^2x[2]^10x[4]^12 - x[1]^10x[3]^2x[4]^12 + x[1]^6x[2]^4x[3]^2x[4]^12
+ x[1]^4x[2]^6x[3]^2x[4]^12 - x[2]^10x[3]^2x[4]^12 + x[1]^6x[2]^2x[3]^4x[4]^12
+ x[1]^4x[2]^4x[3]^4x[4]^12 + x[1]^2x[2]^6x[3]^4x[4]^12 + x[1]^6x[3]^6x[4]^12
+ x[1]^4x[2]^2x[3]^6x[4]^12 + x[1]^2x[2]^4x[3]^6x[4]^12 + x[2]^6x[3]^6x[4]^12
- x[1]^2x[3]^10x[4]^12 - x[2]^2x[3]^10x[4]^12 - x[1]^10x[4]^14 - x[2]^10x[4]^14
- x[3]^10x[4]^14 + x[1]^4x[2]^2x[4]^18 + x[1]^2x[2]^4x[4]^18 + x[1]^4x[3]^2x[4]^18
+ x[1]^2x[2]^2x[3]^2x[4]^18 + x[2]^4x[3]^2x[4]^18 + x[1]^2x[3]^4x[4]^18 + x[2]^2x[3]^4x[4]^18
+ x[1]^4x[4]^20 + x[2]^4x[4]^20 + x[3]^4x[4]^20 - x[1]^2x[4]^22 - x[2]^2x[4]^22
- x[3]^2x[4]^22 - x[4]^24

N=4 Q=3 I=3
D43=x[1]^18 - x[1]^16x[2]^2 - x[1]^14x[2]^4 - x[1]^12x[2]^6 + x[1]^10x[2]^8 + x[1]^8x[2]^10
- x[1]^6x[2]^12 - x[1]^4x[2]^14 - x[1]^2x[2]^16 + x[2]^18 - x[1]^16x[3]^2 - x[1]^12x[2]^4x[3]^2
+ x[1]^10x[2]^6x[3]^2 + x[1]^6x[2]^10x[3]^2 - x[1]^4x[2]^12x[3]^2 - x[2]^16x[3]^2
- x[1]^14x[3]^4 - x[1]^12x[2]^2x[3]^4 + x[1]^10x[2]^4x[3]^4 + x[1]^4x[2]^10x[3]^4
- x[1]^2x[2]^12x[3]^4 - x[2]^14x[3]^4 - x[1]^12x[3]^6 + x[1]^10x[2]^2x[3]^6
- x[1]^6x[2]^6x[3]^6 + x[1]^2x[2]^10x[3]^6 - x[2]^12x[3]^6 + x[1]^10x[3]^8 + x[2]^10x[3]^8
+ x[1]^8x[3]^10 + x[1]^6x[2]^2x[3]^10 + x[1]^4x[2]^4x[3]^10 + x[1]^2x[2]^6x[3]^10
+ x[2]^8x[3]^10 - x[1]^6x[3]^12 - x[1]^4x[2]^2x[3]^12 - x[1]^2x[2]^4x[3]^12 - x[2]^6x[3]^12
- x[1]^4x[3]^14 - x[2]^4x[3]^14 - x[1]^2x[3]^16 - x[2]^2x[3]^16 + x[3]^18 - x[1]^16x[4]^2
- x[1]^12x[2]^4x[4]^2 + x[1]^10x[2]^6x[4]^2 + x[1]^6x[2]^10x[4]^2 - x[1]^4x[2]^12x[4]^2
- x[2]^16x[4]^2 - x[1]^12x[2]^2x[3]^2x[4]^2 + x[1]^10x[2]^4x[3]^2x[4]^2
+ x[1]^4x[2]^10x[3]^2x[4]^2 - x[1]^2x[2]^12x[3]^2x[4]^2 - x[1]^12x[3]^4x[4]^2
+ x[1]^10x[2]^2x[3]^4x[4]^2 - x[1]^6x[2]^6x[3]^4x[4]^2 + x[1]^2x[2]^10x[3]^4x[4]^2
- x[2]^12x[3]^4x[4]^2 + x[1]^10x[3]^6x[4]^2 - x[1]^6x[2]^4x[3]^6x[4]^2
- x[1]^4x[2]^6x[3]^6x[4]^2 + x[2]^10x[3]^6x[4]^2 + x[1]^6x[3]^10x[4]^2
+ x[1]^4x[2]^2x[3]^10x[4]^2 + x[1]^2x[2]^4x[3]^10x[4]^2 + x[2]^6x[3]^10x[4]^2
- x[1]^4x[3]^12x[4]^2 - x[1]^2x[2]^2x[3]^12x[4]^2 - x[2]^4x[3]^12x[4]^2 - x[3]^16x[4]^2
- x[1]^14x[4]^4 - x[1]^12x[2]^2x[4]^4 + x[1]^10x[2]^4x[4]^4 + x[1]^4x[2]^10x[4]^4
- x[1]^2x[2]^12x[4]^4 - x[2]^14x[4]^4 - x[1]^12x[3]^2x[4]^4 + x[1]^10x[2]^2x[3]^2x[4]^4
```

```
- x[1]^6x[2]^6x[3]^2x[4]^4 + x[1]^2x[2]^10x[3]^2x[4]^4 - x[2]^12x[3]^2x[4]^4
+ x[1]^10x[3]^4x[4]^4 - x[1]^6x[2]^4x[3]^4x[4]^4 - x[1]^4x[2]^6x[3]^4x[4]^4
+ x[2]^10x[3]^4x[4]^4 - x[1]^6x[2]^2x[3]^6x[4]^4 - x[1]^4x[2]^4x[3]^6x[4]^4
- x[1]^2x[2]^6x[3]^6x[4]^4 + x[1]^4x[3]^10x[4]^4 + x[1]^2x[2]^2x[3]^10x[4]^4
+ x[2]^4x[3]^10x[4]^4 - x[1]^2x[3]^12x[4]^4 - x[2]^2x[3]^12x[4]^4 - x[3]^14x[4]^4
- x[1]^12x[4]^6 + x[1]^10x[2]^2x[4]^6 - x[1]^6x[2]^6x[4]^6 + x[1]^2x[2]^10x[4]^6
- x[2]^12x[4]^6 + x[1]^10x[3]^2x[4]^6 - x[1]^6x[2]^4x[3]^2x[4]^6 - x[1]^4x[2]^6x[3]^2x[4]^6
+ x[2]^10x[3]^2x[4]^6 - x[1]^6x[2]^2x[3]^4x[4]^6 - x[1]^4x[2]^4x[3]^4x[4]^6
- x[1]^2x[2]^6x[3]^4x[4]^6 - x[1]^6x[3]^6x[4]^6 - x[1]^4x[2]^2x[3]^6x[4]^6
- x[1]^2x[2]^4x[3]^6x[4]^6 - x[2]^6x[3]^6x[4]^6 + x[1]^2x[3]^10x[4]^6 + x[2]^2x[3]^10x[4]^6
- x[3]^12x[4]^6 + x[1]^10x[4]^8 + x[2]^10x[4]^8 + x[3]^10x[4]^8 + x[1]^8x[4]^10
+ x[1]^6x[2]^2x[4]^10 + x[1]^4x[2]^4x[4]^10 + x[1]^2x[2]^6x[4]^10 + x[2]^8x[4]^10
+ x[1]^6x[3]^2x[4]^10 + x[1]^4x[2]^2x[3]^2x[4]^10 + x[1]^2x[2]^4x[3]^2x[4]^10
+ x[2]^6x[3]^2x[4]^10 + x[1]^4x[3]^4x[4]^10 + x[1]^2x[2]^2x[3]^4x[4]^10 + x[2]^4x[3]^4x[4]^10
+ x[1]^2x[3]^6x[4]^10 + x[2]^2x[3]^6x[4]^10 + x[3]^8x[4]^10 - x[1]^6x[4]^12
- x[1]^4x[2]^2x[4]^12 - x[1]^2x[2]^4x[4]^12 - x[2]^6x[4]^12 - x[1]^4x[3]^2x[4]^12
- x[1]^2x[2]^2x[3]^2x[4]^12 - x[2]^4x[3]^2x[4]^12 - x[1]^2x[3]^4x[4]^12 - x[2]^2x[3]^4x[4]^12
- x[3]^6x[4]^12 - x[1]^4x[4]^14 - x[2]^4x[4]^14 - x[3]^4x[4]^14 - x[1]^2x[4]^16 - x[2]^2x[4]^16
- x[3]^2x[4]^16 + x[4]^18
--------------------------------

For I:= 1 To 3 Do
D4i[I]^Q=Subst(C(N,I)+Phi4[I],
[[s[0],Xi(0)],[s[1],Xi(1)],[s[2],Xi(2)],[s[3],Xi(3)]]);
EndFor;
TRUETRUETRUE
--------------------------------
```

Appendix C

The invariants Λ_k^+ and Λ_k^-

In §ap:det con we give the code to test the determinant Conjecture 5.5. Then in §C.2.1 we present an algorithm and code concerning the factors ofΛ_k of Λ_k following the work in Section 5.1. The output for small values of n and q is presented in §C.3. Finally in §C.2.2 we present the code that establishes the coefficients of ξ_{k-1} in the expressions for $\Lambda_k^{\pm}$.

C.1 The code to test Conjecture 5.5

```
N:=3; N1:=N-1; Use SS::=Q[m[1..N,1..N]];
Define M(N) M:=NewMat(N,N);
    For I:=1 To N Do For J:=1 To N
        Do M[I,J]:=m[I,J]
    EndFor EndFor;
Return M EndDefine;
 Mm:=Submat(M(N),2..N1,2..N1); Min:=Minors(N-1,M(N));
MNN:=Min[1]; MN1:=Min[N]; M1N:=Min[N^2-N+1]; M11:=Min[N^2];

Det(M(N))*Det(Mm)=MNN*M11-M1N*MN1;

TRUE
-------------------------------
```

C.2 The $\Lambda_k^{\pm}$

C.2.1 The code to generate the $\Lambda_k^{\pm}$

This code generates the polynomials Λ_k^+ and Λ_k^- such that

$$\Lambda_k^+ \, \Lambda_k^- = \Lambda_k$$

for $k = 2, \ldots, n+2$ utilising the inductive formula given in Lemma 5.11.

Firstly we et up the variables $N = n$ and $Q = q$ and the rings Xi and S within which we work, the ring Xi with generators s[k]=ξ_k with weights $q^k + 1$ and the ring S=$\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ with indeterminates x[i]=x_i. The code below sets $n = 4$ and $q = 3$.

```
--        1)        Preliminaries
--        1a)        Setting up the variables
MEMORY.N:=4; N:=MEMORY.N; MEMORY.N1:=N+1; N1:=MEMORY.N1; N2:=N+2;
MEMORY.Q:=3; Q:=MEMORY.Q; MEMORY.P:=Q; P:=MEMORY.P;

--        1b)        Setting up the ring $\F_q[\xi_0, \xi_1, \dots,  \xi_{n+1},]
W:=NewList(N1+3); W[1]:=1; For I:=0 To N2 Do W[I+2]:=1+Q^I; EndFor;
Use Xi::=Z/(Q)[t,s[0..N2]], Weights(W);
-------------------------------------------------------
```

We define the matrices L(K)=$\mathcal{L}_k$ as defined in Section 5.1, the determinant of which are the polynomials Lambda[K]=Λ_k, and the matrices O(K) as the sub matrix of the matrix L(K+1) with the $k+1$ row and the 1st column removed, the determinant of which are the polynomials Omega[K]=Ω_k,

```
-- 2) Factorisation of Lambda[K] as Lm[K]*Lp[K].
--    2a) Generation of the matrices L(K)and the determinants Lambda[K]=$Lambda_k$.

Define L(I) Q:=MEMORY.Q; M:=NewMat(I,I);
    For K:=0 To I-1 Do  M[1,K+1]:=s[K] EndFor;
    For J:=2 To I Do For K:=0 To J-1 Do M[J,K+1]:=s[J-K-1]^(Q^K) EndFor;
        For K:=J To I-1 Do M[J,K+1]:=s[K-J+1]^(Q^(J-1)) EndFor;
    EndFor;
Return M EndDefine;
Lambda:=NewList(N+2); For K:=1 To N+2 Do Lambda[K]:=Det(L(K)) EndFor;
```

```
Define O(K) K1:=K+1;
    O:=Submat(L(K+1),1..K,2..K1);
Return O EndDefine;
Omega:=NewList(N+2); For K:=1 To N+2 Do Omega[K]:=Det(O(K)) EndFor;
```

We now set Lp0=$\Lambda_0^+ = 1$ and Lm0=$\Lambda_0^- = 1$, Lp as the list of the Λ_k^+ and Lm as the list of the Λ_k^- for $k = 1, \ldots, n+1$. Then the $\Lambda_4^\pm$ are generated following the algorithm of Lemma 5.11:

Initially we set

$$\mathrm{Lp}[1] = \Lambda_1^+ = 1 \quad \text{and} \quad \mathrm{Lm}[1] = \Lambda_1^- = \xi_0$$

$$\mathrm{Lp}[2] = \Lambda_2^+ = \Lambda_1^{\frac{q+1}{2}} + \Omega_1 = \xi_0^{\frac{q+1}{2}} + \xi_1 \quad \text{and} \quad \mathrm{Lp}[2] = \Lambda_2^+ = \Lambda_1^{\frac{q+1}{2}} - \Omega_1 = \xi_0^{\frac{q+1}{2}} - \xi_1$$

We calculate the subsequent Lp[K]=Λ_k^+ and Lm[K]=Λ_k^- for $k = 3, \ldots, n+1$ using the inductive formulae

$$\Lambda_k^+ = \frac{(\Lambda_{k-1}^+)^{\frac{q+1}{2}} + \Omega_{k-1}^+}{(\Lambda_{k-2}^+)^q} \quad \text{and} \quad \Lambda_k^- = \frac{(\Lambda_{k-1}^+)^{\frac{q+1}{2}} - \Omega_{k-1}^+}{(\Lambda_{k-2}^-)^q}$$

when $q \equiv 3 \bmod 4$ and

$$\Lambda_k^+ = \frac{(\Lambda_{k-1}^+)^{\frac{q+1}{2}} + \Omega_{k-1}^+}{(\Lambda_{k-2}^-)^q} \quad \text{and} \quad \Lambda_k^- = \frac{(\Lambda_{k-1}^+)^{\frac{q+1}{2}} - \Omega_{k-1}^+}{(\Lambda_{k-2}^+)^q}$$

when $q \equiv 1 \bmod 4$

```
-- 2b) Generation of the factors Lp[K]=$\Lambda_k^+$ and Lm[K]=$\Lambda_k^-$ of Lambda[K]

Lp0:=1; Lm0:=1;
Lp:=NewList(N2); Lm:=NewList(N2); Qq:=(Q+1)/2;
Lp[1]:=1; Lm[1]:=s[0];
Lp[2]:=Lambda[1]^Qq+Omega[1]; Lm[2]:=Lambda[1]^Qq-Omega[1];

For K:=2 To N+1 Do
    If Mod(Q,4)=3 Then
        Lp[K+1]:=(Lambda[K]^Qq+Omega[K])/(Lp[K-1])^Q; --PrintLn Lp[K+1];
        Lm[K+1]:=(Lambda[K]^Qq-Omega[K])/(Lm[K-1])^Q; --PrintLn Lm[K+1];
    Elsif Mod(Q,4)=1 Then
        If K<N+1 Then
            Lp[K+1]:=(Lambda[K]^Qq+Omega[K])/(Lm[K-1])^Q; --PrintLn Lp[K+1];
            Lm[K+1]:=(Lambda[K]^Qq-Omega[K])/(Lp[K-1])^Q; --PrintLn Lm[K+1];
EndIf EndIf EndFor;
```

We check that $\Lambda_k = \Lambda_k^+ \, \Lambda_k^-$ for each $k = 1, \ldots, n+1$ and that the expressions for each of the $\lambda_k^{\pm}$ are in fact polynomials.

```
-- 2c) Checking that each Lambda[K]=Lp[K]*Lm[K] and that the factors are polynomials.


PrintLn; PrintLn 'Q=',Q;
PrintLn '2: Lambda[K]=Lp[K]*Lm[K]?'; PrintLn 'Type of the Lp[K], Lm[K]';
For K:=1 To N+2 Do
    If Mod(Q,4)=3 Or K<N+2 Then
        If Lp[K]*Lm[K]=Lambda[K] Then PrintLn 'Lp[',K,']*Lm[',K,']=Lambda[',K,']' EndIf;
    Type(Lp[K]);Type(Lm[K]); PrintLn; PrintLn
EndIF EndFor;
```

C.2.2 The code to check Lemma 5.12

The following code ascertains the coefficient of s[K-1]=ξ_{k-1} in the expressions for Lp[K]=Λ_k^+ and for Lm[K]=Λ_k^- generated using the code in the previous section. Thus the code was used to check Lemma 5.12 for small values of n and q.

```
-- 3) Checking the conjecture regarding the coefficients of s[N-1]=$\xi_{n-1}$
--in the $\Lambda_n^\pm$


PrintLn '3: Checking the coefficient conjecture';
For K:=2 To N+1 Do
  If Mod(Q,4)=3 Or K<N+1 Then Cp:=Coefficients(Lp[K+1],s[K]); Cm:=Coefficients(Lm[K+1],s[K]);
  If Cp[1]=Lp[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lp[',K+1,'] is Lp[',K-1,']^Q'
    ElsIf Cp[1]=-Lp[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lp[',K+1,'] is -Lp[',K-1,']^Q'
    ElsIf Cp[1]=Lm[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lp[',K+1,'] is Lm[',K-1,']^Q'
    ElsIf Cp[1]=-Lm[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lp[',K+1,'] is -Lm[',K-1,']^Q'
    EndIf;
  If Cm[1]=Lm[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lm[',K+1,'] is Lm[',K-1,']^Q'
    ElsIf Cm[1]=-Lm[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lm[',K+1,'] is -Lm[',K-1,']^Q'
    ElsIf Cm[1]=Lp[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lm[',K+1,'] is Lp[',K-1,']^Q'
    ElsIf Cm[1]=-Lp[K-1]^Q Then PrintLn'Coefficient of s[',K,'] in Lm[',K+1,'] is -Lp[',K-1,']^Q'
EndIf; PrintLn EndIf EndFor;
```

C.3 Output from the code for $n = 4$

Here we have an example of the case $q \equiv 3 \bmod 4$.

```
 ------------------------------
Q=3
------------------------------
2: Lambda[K]=Lp[K]*Lm[K]?
------------------------------
Type of the Lp[K], Lm[K]
------------------------------
Lp[1]*Lm[1]=Lambda[1]
INTPOLY
Lp[2]*Lm[2]=Lambda[2]
POLYPOLY
Lp[3]*Lm[3]=Lambda[3]
POLYPOLY
Lp[4]*Lm[4]=Lambda[4]
POLYPOLY
Lp[5]*Lm[5]=Lambda[5]
POLYPOLY
Lp[6]*Lm[6]=Lambda[6]
POLYPOLY
------------------------------
3: Checking the coefficient conjecture
------------------------------
Coefficient of s[2] in Lp[3] is -Lm[1]^Q
Coefficient of s[2] in Lm[3] is Lp[1]^Q
Coefficient of s[3] in Lp[4] is Lm[2]^Q
Coefficient of s[3] in Lm[4] is -Lp[2]^Q
Coefficient of s[4] in Lp[5] is -Lm[3]^Q
Coefficient of s[4] in Lm[5] is Lp[3]^Q
Coefficient of s[5] in Lp[6] is Lm[4]^Q
Coefficient of s[5] in Lm[6] is -Lp[4]^Q
```

Here we have an example of the case $q \equiv 1 \bmod 4$.

```
------------------------------
Q=5
------------------------------
2: Lambda[K]=Lp[K]*Lm[K]?
------------------------------
Type of the Lp[K], Lm[K]
------------------------------
Lp[1]*Lm[1]=Lambda[1]
INTPOLY
Lp[2]*Lm[2]=Lambda[2]
POLYPOLY
Lp[3]*Lm[3]=Lambda[3]
POLYPOLY
Lp[4]*Lm[4]=Lambda[4]
POLYPOLY
Lp[5]*Lm[5]=Lambda[5]
POLYPOLY
------------------------------
3: Checking the coefficient conjecture
------------------------------
Coefficient of s[2] in Lp[3] is -Lp[1]^Q
Coefficient of s[2] in Lm[3] is Lm[1]^Q
Coefficient of s[3] in Lp[4] is Lp[2]^Q
Coefficient of s[3] in Lm[4] is -Lm[2]^Q
Coefficient of s[4] in Lp[5] is -Lp[3]^Q
Coefficient of s[4] in Lm[5] is Lm[3]^Q
```

Appendix D

The factors of the $\Lambda_n^{\pm}$ and $\Lambda_{n+1}^{\pm}$ in $\mathbb{F}_q[x_1, \ldots, x_n]$

D.1 CoCoA code to factorise $\Lambda_n^{\pm}$ and $\Lambda_{n+1}^{\pm}$

The code given below is for the case $n = 4, q = 3, \varepsilon = 1$ so the quadratic form ξ_0 is Q_s.

- Setting up the variables and rings: This code is given in Appendix C.2.1
- Calculating the non square elements of $\mathbb{F}_q^*$

```
-- Finding a non square element, Nu, of Fq

Sq:=NewList((Q-1)/2); NSq:=NewList((Q-1)/2); Count:=1;
For I:=1 To (Q-1)/2 Do Sq[I]:=Mod(I^2,Q) EndFor;
For I:=1 To Q-1 Do If Not I IsIn Sq Then NSq[Count]:=I; Count:=Count+1 EndIf EndFor;
Nu:=NSq[1];
-- Put Ep:= 1 or Ep:=Nu here for S or N type of form
Ep:=1; MEMORY.Ep:=Ep;
PrintLn; PrintLn'N=',N,'  Q=',Q,'  Ep=',Ep;
```

- Generation of the $\Lambda_k^{\pm}$: This code is given in Appendix C.2.1.
- The map from $\mathbb{F}_q[\xi_0, \ldots, \xi_{n-1}]$ to $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$

```
-- Defining the map from the ring Xi to the ring S
Define Qmap(N) Ep:=MEMORY.Ep; Q:=MEMORY.Q;
    Qlist:=NewList(N+4); Qlist[1]:=t;
    For J:=0 To N+2 Do Xi:=Ep*x[1]^(Q^J+1);
```

```
        For I:=2 To N Do Xi:=Xi+x[I]^(Q^J+1) EndFor; Qlist[J+2]:=Xi;
    EndFor; Qmap:=RMap(Qlist);
Return Qmap EndDefine;
Use S;
XLambda:=Image(Lambda[N],Qmap(N)); XLp:=Image(Lp[N],Qmap(N)); XLm:=Image(Lm[N],Qmap(N));
-- XLambda=XLp*XLm;
XLp1:=Image(Lp[N+1],Qmap(N)); XLm1:=Image(Lm[N+1],Qmap(N));
```

- Generation of the polynomials of products of monic vectors $\overline{\mathcal{V}}, \overline{\mathcal{Z}}, \overline{\mathcal{S}}, \overline{\mathcal{N}}$.

  These are the polynomials as described in section 5.4.1, generated as VPol, ZPol, SPol, and NPol respectively.

```
-- Generation of the polyomial VPol
VPol:=1;
For V1:=0 To Q-1 Do For V2:=0 To Q-1 Do For V3:=0 To Q-1 Do For V4:=0 To Q-1 Do
    If V1=1 Or V1=0 And V2=1 Or V1=0 And V2=0 And V3=1
        Or V1=0 And V2=0 And V3=0 And V4=1 Then
        V:=V1*x[1]+V2*x[2]+V3*x[3]+V4*x[4]; VPol:=VPol*V
EndIf EndFor EndFor EndFor EndFor;
Ell:=-VPol;
--If XLambda=Ep*Ell^2 Then PrintLn'TRUE: XLambda=Ep*Ell^2' EndIf;
-------------------------------------------------------
--Generation of the polynimials SPol, NPol and ZPOl
ZPol:=1; SqPol:=1; NSqPol:=1;
For V1:=0 To 1 Do For V2:=0 To Q-1 Do For V3:=0 To Q-1 Do For V4:=0 To Q-1 Do
    If V1=1 Or V1=0 And V2=1 Or V1=0 And V2=0 And V3=1
        Or V1=0 And V2=0 And V3=0 And V4=1 Then
        Qv:= Mod(Ep*V1^2+V2^2+V3^2+V4^2,Q);
        If V1=1 Then Xv:=(Ep*V1*x[1]+V2*x[2]+V3*x[3]+V4*x[4])/Ep
            Else Xv:=Ep*V1*x[1]+V2*x[2]+V3*x[3]+V4*x[4] EndIf;
        If Qv=0 Then ZPol:=ZPol*Xv
            Elsif Qv IsIn Sq Then SqPol:=SqPol*Xv
            Elsif Qv IsIn NSq Then NSqPol:=NSqPol*Xv
EndIf EndIf EndFor EndFor EndFor EndFor;
-- If ZPol*SqPol*NSqPol/VPol=1 Then PrintLn 'TRUE: ZPol*SqPol*NSqPol=VPol' EndIf;
```

- The factorisation of $\Lambda_n^{\pm}$ and $\Lambda_{n+1}^{\pm}$ over $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.

  We test to see whether the each of $\Lambda_n^{\pm}$ is a multiple of $\overline{\mathcal{Z}}\ \overline{\mathcal{S}}^2$ or $\overline{\mathcal{Z}}\ \overline{\mathcal{N}}^2$ and whether each of $\Lambda_{n+1}^{\pm}$ is either zero or a multiple of $\overline{\mathcal{Z}}\ \overline{\mathcal{S}}^{q+1}\ \overline{\mathcal{N}}^{q+1}$.

```
ProdS:=ZPol*SqPol^2; ProdN:=ZPol*NSqPol^2;
QuotpS:=XLp/ProdS; QuotpN:=XLp/ProdN;
If Type(QuotpS)=POLY Then PrintLn'XLp=',QuotpS,'*ZPol*SqPol^2' EndIf;
If Type(QuotpN)=POLY Then PrintLn'XLp=',QuotpN,'*ZPol*NSqPol^2' EndIf;
QuotmS:=XLm/ProdS; QuotmN:=XLm/ProdN;
If Type(QuotmS)=POLY Then PrintLn'XLm=',QuotmS,'*ZPol*SqPol^2' EndIf;
If Type(QuotmN)=POLY Then PrintLn'XLm=',QuotmN,'*ZPol*NSqPol^2' EndIf;

ProdSN:=ZPol*SqPol^(Q+1)*NSqPol^(Q+1);
If XLp1=0 Then PrintLn 'XLp1=0' Else Quot:=XLp1/ProdSN;
    If Type(Quot)=POLY Then PrintLn'XLp1=',Quot,'*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)'
EndIf EndIf;
If XLm1=0 Then PrintLn 'XLm1=0' Else Quot:=XLm1/ProdSN;
    If Type(Quot)=POLY Then PrintLn'XLm1=',Quot,'*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)'
EndIf EndIf;
```

D.2 Output from the code

D.2.1 Output for the case n=2

- The quadratic form Q_s with ε a square.

```
N=2  Q=3  Ep=1
XLp=-1*ZPol*NSqPol^2
XLm=-1*ZPol*SqPol^2
XLp1=-1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
------------------------------
N=2  Q=5  Ep=1
XLp=2*ZPol*NSqPol^2
XLm=-2*ZPol*SqPol^2
XLp1=2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
------------------------------
N=2  Q=7  Ep=1
XLp=2*ZPol*NSqPol^2
XLm=-3*ZPol*SqPol^2
XLp1=2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
------------------------------
N=2  Q=11  Ep=1
XLp=2*ZPol*NSqPol^2
XLm=-5*ZPol*SqPol^2
XLp1=2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
------------------------------
N=2  Q=13  Ep=1
XLp=2*ZPol*NSqPol^2
XLm=-6*ZPol*SqPol^2
XLp1=2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
------------------------------
N=2  Q=17  Ep=1
XLp=2*ZPol*NSqPol^2
XLm=-8*ZPol*SqPol^2
```

```
XLp1=2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
```

- The quadratic form Q_n with ε a non square.

```
N=2  Q=3  Ep=2
XLp=1*ZPol*SqPol^2
XLm=-1*ZPol*NSqPol^2
XLp1=0
XLm1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=2  Q=5  Ep=2
XLp=2*ZPol*SqPol^2
XLm=1*ZPol*NSqPol^2
XLp1=0
XLm1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=2  Q=7  Ep=3
XLp=3*ZPol*SqPol^2
XLm=1*ZPol*NSqPol^2
XLp1=0
XLm1=-2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=2  Q=11  Ep=2
XLp=5*ZPol*SqPol^2
XLm=-4*ZPol*NSqPol^2
XLp1=0
XLm1=-2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=2  Q=13  Ep=2
XLp=6*ZPol*SqPol^2
XLm=-4*ZPol*NSqPol^2
XLp1=0
XLm1=-4*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=2  Q=17  Ep=3
XLp=8*ZPol*SqPol^2
XLm=-6*ZPol*NSqPol^2
XLp1=0
```

```
XLm1=-6*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
```

D.2.2 Output for the case $n = 3$

- The quadratic form Q_s with ε a square.

```
N=3  Q=3  Ep=1
-------------------------------
XLp=2*ZPol*NSqPol^2
XLm=-1*ZPol*SqPol^2
XLp1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
-------------------------------
N=3  Q=5  Ep=1
-------------------------------
XLp=2*ZPol*NSqPol^2
XLm=-2*ZPol*SqPol^2
XLp1=4*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
-------------------------------
N=3  Q=7  Ep=1
-------------------------------
XLp=2*ZPol*NSqPol^2
XLm=-3*ZPol*SqPol^2
XLp1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
-------------------------------
N=3  Q=11  Ep=1
-------------------------------
XLp=2*ZPol*NSqPol^2
XLm=-5*ZPol*SqPol^2
XLp1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
-------------------------------
N=3  Q=13  Ep=1
-------------------------------
XLp=2*ZPol*NSqPol^2
XLm=-6*ZPol*SqPol^2
```

```
XLp1=4*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
```

- The quadratic form Q_n with ε a non square.

```
N=3  Q=3  Ep=2
-------------------------------
XLp=-1*ZPol*SqPol^2
XLm=1*ZPol*NSqPol^2
XLp1=0
XLm1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=3  Q=5  Ep=2
-------------------------------
XLp=2*ZPol*SqPol^2
XLm=1*ZPol*NSqPol^2
XLp1=0
XLm1=-2*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=3  Q=7  Ep=3
-------------------------------
XLp=2*ZPol*SqPol^2
XLm=-2*ZPol*NSqPol^2
XLp1=0
XLm1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=3  Q=11  Ep=2
-------------------------------
XLp=-1*ZPol*SqPol^2
XLm=-2*ZPol*NSqPol^2
XLp1=0
XLm1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
-------------------------------
N=3  Q=13  Ep=2
-------------------------------
XLp=6*ZPol*SqPol^2
XLm=-4*ZPol*NSqPol^2
XLp1=0
XLm1=-5*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
```

D.2.3 Output for the case $n = 4$

- The quadratic form Q_s with ε a square.

```
------------------------------
N=4  Q=3  Ep=1
------------------------------
XLp=1*ZPol*NSqPol^2
XLm=1*Z*Pol*SqPol^2
XLp1=1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
XLm1=0
------------------------------
N=4  Q=5  Ep=1
------------------------------
XLp=-1*ZPol*NSqPol^2
XLm=-1*Z*Pol*SqPol^2
```

- The quadratic form Q_n with ε a non square.

```
------------------------------
N=4  Q=3  Ep=2
------------------------------
XLp=-1*ZPol*SqPol^2
XLm=1*ZPol*NSqPol^2
XLp1=0
XLm1=-1*ZPol*SqPol^(Q+1)*NSqPol^(Q+1)
------------------------------
------------------------------
N=4  Q=5  Ep=2
------------------------------
XLp=-1*ZPol*SqPol^2
XLm=-2*ZPol*NSqPol^2
------------------------------
```

Appendix E

Alternative generation of the d_i invariants

E.1 The code to generate new invariants from the Λ_k polynomials

This code implements the algorithm outlined in Chapter 6 in the case $n = 4$, $q = 3$ and $\xi_0 = Q_s = x_1^2 + x_2^2 + x_3^2 + x_4^2$. First we set up the variables and rings and generate the $\Lambda_k^{\pm}$. The code is given in Appendix C and uses the notation Lp[K] and Lm[K] for Λ_k^+ and Λ_k^- respectively.

We then define the Total Steenrod Operation is presented in Lemma 3.13.

```
--4) Calculating the Total Steenrod Operation on Lp[K] and Lm[K] for k=1,... n
--4a) Defining the Total Steenrod Operation, TSO, on the s[k]

Define TSO(X) N:=MEMORY.N; Q:=MEMORY.Q; S1:=NewMat(N+2,2);
    S1[1,1]:=s[0]; S1[1,2]:=s[0]-2s[1]+s[0]^3;
    For I:=1 To N Do S1[I+1,1]:=s[I];S1[I+1,2]:=s[I]-s[I-1]^Q-s[I+1]+s[I]^Q EndFor;
    S1[N+2,1]:=s[N+1]; S1[N+2,2]:=s[N+1]-s[N]^Q+s[N+1]^Q; S2:=Subst(X,S1);
Return S2 EndDefine;

--4b) Calculating the Total Steenrod Operation on each of the Lp[K] and Lm[K],
--k=1, ..., n , denoting by Sp[k] and Sm[K] the operation on Lp[K] and Lm[K].

Sp0:=TSO(Lp0);Sm0:=TSO(Lm0); Sp:=NewList(N1); Sm:=NewList(N1);
For K:=1 To N Do Sp[K]:=TSO(Lp[K]); Sm[K]:=TSO(Lm[K] EndFor;
```

The specializations of $\mathbb{F}_q[\xi_0, \xi_1, \ldots, \xi_n]$ to $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ are the ring homomorphisms deter-

mined by the choice of quadratic form ξ_0. When $\xi_0 \sim Q_+$ the map is denoted Qpmap(N) and when $\xi_0 \sim Q_-$ denoted Qmmap(N).

When $n = 4$ these are the maps $Q^{\sigma}_{k,k}$ and $Q^{\nu}_{k,k}$ respectively, as presented in Definition 6.1, as in this case $Q_+ \sim Q_s$ and $Q_- \sim Q_n$.

```
--5) Setting up the map from Xi to S defined by the quadratic form s[0].
--5a) Defining the map Qpmap(N), containing the image of the Xi variables
--under the map defined by the quadratic form s[0] of plus type

Define Qpmap(K) N:=MEMORY.N; Q:=MEMORY.Q; Qp:=NewList(N+3); Ep:=1; Qp[1]:=t;
    For J:=0 To N+1 Do Xi:=Ep*x[1]^(Q^J+1); For I:=2 To K Do Xi:=Xi+x[I]^(Q^J+1) EndFor;
    Qp[J+2]:=Xi; EndFor; Qpmap:=RMap(Qp);
Return Qpmap EndDefine;

--5b)  Defining the map Qmmap(N) as 5a) but with s[0] of minus type, Ep is a non square.

Define Qmmap(K) N:=MEMORY.N; Q:=MEMORY.Q; Qm:=NewList(N+3); Ep:=-1; Qm[1]:=t;
    For J:=0 To N+1 Do Xi:=Ep*x[1]^(Q^J+1); For I:=2 To K Do Xi:=Xi+x[I]^(Q^J+1) EndFor;
    Qm[J+2]:=Xi; EndFor; Qmmap:=RMap(Qm);
Return Qmmap EndDefine;
```

Testing the conjecture regrding elements of the kernels of the above maps

```
--6) Testing the conjecture regarding the kernel of the maps Qpmap and Qmmap
Use S;
For K:=2 To 4 Do PrintLn 'K=',K; If K=2 Then
    Image(Lm[K-1]^3*Sp[K]-Lp[K+1]*Sm0^3,Qmmap(K-1));
    mage(Lm[K-1]^3*Sm[K]+Lp[K+1]*Sp0^3,Qpmap(K-1));
    Image(Lp[K-1]^3*Sp[K]+Lm[K+1]*Sm0^3,Qmmap(K-1));
    Image(Lp[K-1]^3*Sm[K]-Lm[K+1]*Sp0^3,Qpmap(K-1));
    Else
    Image(Lm[K-1]^3*Sp[K]-Lp[K+1]*Sm[K-2]^3,Qmmap(K-1));
    Image(Lm[K-1]^3*Sm[K]+Lp[K+1]*Sp[K-2]^3,Qpmap(K-1));
    Image(Lp[K-1]^3*Sp[K]+Lm[K+1]*Sm[K-2]^3,Qmmap(K-1));
    Image(Lp[K-1]^3*Sm[K]-Lm[K+1]*Sp[K-2]^3,Qpmap(K-1));
EndIf; PrintLn EndFor;
-----------------------------------------------------------------------
```

Calculating invariants with reference to Conjecture 6.12.

```
-- 7) Calculating invariants: dividing elements of the kernel of the Qpmap and Qmmap.
--        Divisibilty of expressions is checked by checking type.

Use Xi;
PrintLn 'Generation and type of the Bp[I], Bm[I], Cp[I], Cm[I]';
For I:=1 To N Do
    Bp:=NewList(N); Cp:=NewList(N); Bm:=NewList(N); Cm:=NewList(N);
    If I=1 Then Um:=Lm0; Up:=Lp0 Else Um:=Lm[I-1]; Up:=Lp[I-1] EndIf;
    Sm:=TSO(Um); Sp:=TSO(Up);
    If I=1 Then Vm:=1; Vp:=1 Elsif I=2 Then
        Vm:=TSO(Lm0^3); Vp:=TSO(Lp0^3)
        Else Vm:=TSO(Lm[I-2]^3); Vp:=TSO(Lp[I-2]^3)
    EndIf; PrintLn 'I=',I;
    Bp[I]:=(Up^3*TSO(Lp[I])+Lm[I+1]*Vm)/Lp[I]/Sp;Type(Bp[I]);
    Cp[I]:=(Up^3*TSO(Lm[I])-Lm[I+1]*Vp)/Lm[I]/Sp;Type(Cp[I]);
    Bm[I]:=(Um^3*TSO(Lm[I])+Lp[I+1]*Vp)/Lm[I]/Sm;Type(Bm[I]);
    Cm[I]:=(Um^3*TSO(Lp[I])-Lp[I+1]*Vm)/Lp[I]/Sm;Type(Cm[I]);
    PrintLn;
EndFor;

-----------------------------------------------------------------
```

The invariants d^+ and d^- are generated from the matrix $S_n(X)$ defined in section 6.2.

The matrices are adjusted by removing the s[k] terms.

```
--7) Defining the invariants Dm and Dp
--7a) Defining the matrix S_n(X) as St(K), the dummy variable t is used for $X$.

Define St(K) Q:=MEMORY.Q; M:=NewMat(K+1,K+1);
    For I:=1 To K Do M[1,I]:=s[I-1] EndFor; M[1,K+1]:=t;
    For J:=2 To K+1 Do For I:=0 To J-1 Do M[J,I+1]:=s[J-I-1]^(Q^I) EndFor;
    For I:=J To K-1 Do M[J,I+1]:=s[I-J+1]^(Q^(J-1)) EndFor;
    M[J,K+1]:=t^(Q^(J-1)); EndFor;
    Return M
EndDefine;

-----------------------------------------------------------------

--7b) Defining adjusted matrices Mm(I) and Mp(I) being the
```

```
--St[k] matrices from which the s[k] terms have been removed.
--The dummy variable t is set to 1.

Define Mp(K) Q:=MEMORY.Q; Lp:=MEMORY.Lp;Lp0:=MEMORY.Lp0; Lm:=MEMORY.Lm;Lm0:=MEMORY.Lm0;
    M:=Subst(St(K),t,1);
    If K=1 Then U:=Lm0^Q Else U:=Lm[K-1]^Q EndIf;
    For I:=0 To K Do  M[I+1,1]:=M[I+1,1]*U; EndFor;
    M[K+1,1]:=M[K+1,1]-(-1)^K*Lp[K+1];
Return M EndDefine;

Define Mm(K) Q:=MEMORY.Q; Lp:=MEMORY.Lp;Lp0:=MEMORY.Lp0; Lm:=MEMORY.Lm;Lm0:=MEMORY.Lm0;
    M:=Subst(St(K),t,1);
    If K=1 Then U:=Lp0^Q Else U:=Lp[K-1]^Q EndIf;
    For I:=0 To K Do M[I+1,1]:=M[I+1,1]*U; EndFor; M[K+1,1]:=M[K+1,1]+(-1)^K*Lm[K+1];
Return M EndDefine;

--For I:=1 To N Do PrintLn 'Mm(',I,')=',Mm(I);PrintLn 'Mp(',I,')=',Mp(I) EndFor;
-----------------------------------------------------------------------

-- 7c) Generating the invariants  Dm[I] and Dp[I]:
--       by dividing out Lambda[I] and TSO(Lm[1]) or TSO(Lp[I]) from the determinants of the
--       Mp(I) and Mm(I) respectively.

Dm:=NewList(N); Dp:=NewList(N);
Dm[1]:=Det(Mm(1))/Lambda[1]/Sp0; Dp[1]:=Det(Mp(1))/Lambda[1]/Sm0;

For I:=2 To N Do
    Dm[I]:=Det(Mm(I))/Lambda[I]/Sp[I-1]; Dp[I]:=Det(Mp(I))/Lambda[I]/Sm[I-1];
EndFor;

--7d) Checking that the Dm(I) and Dp(I) are polynomials.

PrintLn 'Type of the Dm(I) and Dp(I)';
For I:=1 To N Do PrintLn; PrintLn 'I=',I; Type(Dm[I]); Type(Dp[I]) EndFor;
-----------------------------------------------------------------------
```

Introducing a dummy variable into the Total Steenrod Operation and $M_k^{\pm}$.

```
--8) Working with a dummy variable
```

```
--8a) Defining the Total Steenrod Operation with dummy variable

Define TSOt(X)N:=MEMORY.N; Q:=MEMORY.Q; Nn:=N+1; S1:=NewMat(N+1,2);
    S1[1,1]:=s[0]; S1[1,2]:=s[0]*t^4-2s[1]*t^2+s[0]^3;
    For I:=1 To N Do S1[I+1,1]:=s[I];
        S1[I+1,2]:=s[I]*t^(2*(Q^I+1))-s[I-1]^Q*t^(2*Q^I)-s[I+1]*t^2+s[I]^Q; EndFor;
    S2:=Subst(X,S1);
Return S2 EndDefine;

--8b) Defining the augmented matrices with dummy variable Mmt(I) and Mpt(I)

Define Mpt(K) Q:=MEMORY.Q; Lp:=MEMORY.Lp;Lp0:=MEMORY.Lp0; Lm:=MEMORY.Lm;Lm0:=MEMORY.Lm0;
    M:=St(K); If K=1 Then U:=Lm0^Q Else U:=Lm[K-1]^Q EndIf;
    For I:=0 To K Do M[I+1,1]:=M[I+1,1]*U; EndFor;
    M[K+1,1]:=M[K+1,1]-(-1)^K*Lp[K+1];
Return M EndDefine;

Define Mmt(K) Q:=MEMORY.Q; Lp:=MEMORY.Lp;Lp0:=MEMORY.Lp0; Lm:=MEMORY.Lm;Lm0:=MEMORY.Lm0;
    M:=St(K); If K=1 Then U:=Lp0^Q Else U:=Lp[K-1]^Q EndIf;
    For I:=0 To K Do M[I+1,1]:=M[I+1,1]*U; EndFor;
    M[K+1,1]:=M[K+1,1]+(-1)^K*Lm[K+1];
Return M EndDefine;
-----------------------------------------------------------------
```

Generating the Chern polynomials as defined in §3.3 so that we can check the new invariants against the Chern Orbit classes.

```
-- 9) Defining the Chern polynomials for quadratic form of plus or minus type
--         depending on the input value Ep as 1 or a non square.
Define ChCo(K,Ep) N:=4; P:=MEMORY.P; Q:=MEMORY.Q; Ch:=1;
    For A1:=0 To Q-1 Do For A2:=0 To Q-1 Do For A3:=0 To Q-1 Do For A4:=0 To Q-1 Do
        Xi:=Ep*A1^2+A2^2+A3^2+A4^2;
        If Mod(Xi,P)=K Then X:=Ep*A1*x[1]+A2*x[2]+A3*x[3]+A4*x[4]; Ch:=Ch*(t-X); EndIf;
    EndFor EndFor EndFor EndFor;--PrintLn 'Degree of poly is ',Deg(Ch);
    ChCo:=Coefficients(Ch,t);
Return ChCo; EndDefine;
-----------------------------------------------------------------
```

Implementing the algorithm for $\xi_0 = Q_s$ that is using the plus type map Qpmap. Thcode can also be implemeted for $\xi_0 = Q_n$ using the minus type map qmmap.

```
-- 10) Implementing the algorithm for N=4 : Dimension 4 Plus type map with dummy variable
--     10a) Generation of the invariants:
            -- Dp the reduced determinant of the augmented matrix Mpt(N)
            -- Bp and Cp from section 6. (Noting that Dp^2=Bp*Cp)
Use Xi;
PrintLn; PrintLn 'Plus Type';
Dp:=Det(Mmt(N))/Lambda[N]/TSOt(Lp[N-1])/t; -- Dp; Type(Dp);
Bp:=(Lp[N-1]^3*TSOt(Lp[N])+t^2*Lm[N+1]*TSOt(Lm[N-2]^3))/Lp[N]/TSOt(Lp[N-1]); --Bp; Type(Bp);
Cp:=(Lp[N-1]^3*TSOt(Lm[N])-t^2*Lm[N+1]*TSOt(Lp[N-2]^3))/Lm[N]/TSOt(Lp[N-1]); --Cp; Type(Cp);
-- If Dp^2=Bp*Cp Then PrintLn 'Dp^2=Bp*Cp' Else PrintLn 'False that Dp^2=Bp*Cp' EndIf;

-----------------------------------------------------------------

-- 10b) Finding new invariants from Bp/Dp.
        -- The rational expression Bp/Dp cancels the common factors from Bp and Dp
        -- so we proceed using the numerator and denominator
        -- The coefficients of t in the numerator and denomiantor are found
        -- In particular we take the coefficients of degrees q^{n-1}-q^{n-2}
        -- and q^{n-1}-q^{n-3} being the degrees of qth roots of the C(N,I) invariants

BDp:=Bp/Dp; Ep:=Num(BDp); Fp:=Den(BDp); -- Type(BDp); Ep^2=Bp; Ep*Fp=Dp;  Fp^2=Cp;

CEp:=Coefficients(Ep,t);
For I:=1 To Len(CEp) Do If NOT Den(CEp[I]/Lp[N-1])=1 Then
    PrintLn 'Coefficient of t^',Len(CEp)-I,' is: ',CEp[I] EndIf
EndFor;
DELp3:=CEp[19]; DELp2:=CEp[25]; -- DELp2; DELp3;

CFp:=Coefficients(Fp,t);
For I:=1 To Len(CFp) Do If NOT Den(CFp[I]/Lp[N-1])=1 Then
    PrintLn 'Coefficient of t^',Len(CFp)-I,' is: ',CFp[I] EndIf
EndFor;
DFLp3:=CFp[19]; DFLp2:=CFp[25]; -- DFLp2; DFLp3;
-----------------------------------------------------------------

--10c) Mapping the Ep and Fp invariants to the ring S and dividing by factor Lp[N-1].

Use S;
```

```
DELp3Ip:=Image(DELp3,Qpmap(4)); DELp2Ip:=Image(DELp2,Qpmap(4));
LpIp:=Image(Lp[N-1],Qpmap(4));
DEp3:=DELp3Ip/LpIp; DEp2:=DELp2Ip/LpIp;

DFLp3Ip:=Image(DFLp3,Qpmap(4)); DFLp2Ip:=Image(DFLp2,Qpmap(4));
LpIp:=Image(Lp[N-1],Qpmap(4));
DFp3:=DFLp3Ip/LpIp; DFp2:=DFLp2Ip/LpIp;
-----------------------------------------------------------------

--10d) Checking the relation between the new found invariants and the Chern orbit classes

ChCo2p:=ChCo(2,1); ChCo1p:=ChCo(1,1);

If DEp2=ChCo2p[25] Then PrintLn 'DEp2=ChCo2p[25]' EndIf;
If DEp3=ChCo2p[19] Then PrintLn 'DEp3=ChCo2p[19]' EndIf;

If DFp2=ChCo1p[25] Then PrintLn 'DFp2=ChCo1p[25]' EndIf;
If DFp3=ChCo1p[19] Then PrintLn 'DFp3=ChCo1p[19]' EndIf;
-----------------------------------------------------------------

-- 10d) Alternative for minus type map

ChCo2m:=ChCo(2,-1); ChCo1m:=ChCo(1,-1);

If DEm2=ChCo2m[25] Then PrintLn 'DEm2=ChCo2m[25]' EndIf;
If DEm3=ChCo2m[19] Then PrintLn 'DEm3=ChCo2m[19]' EndIf;

If DFm2=ChCo1m[25] Then PrintLn 'DFm2=ChCo1m[25]' EndIf;
If DFm3=ChCo1m[19] Then PrintLn 'DFm3=ChCo1m[19]' EndIf;
```

E.2 CoCoA output: generation of invariants when n=4 and q=3

We give the output for the plus type and minus type maps

```
Testing elements of the kernels of the restriction of the Qpmap(k-1), Qmmap(k-1)
-------------------------------
Image(Lm[K-1]^3*Sp[K]-Lp[K+1]*Sm[K-2]^3,Qmmap(K-1))
Image(Lm[K-1]^3*Sm[K]+Lp[K+1]*Sp[K-2]^3,Qpmap(K-1))
Image(Lp[K-1]^3*Sp[K]+Lm[K+1]*Sm[K-2]^3,Qmmap(K-1))
Image(Lp[K-1]^3*Sm[K]-Lm[K+1]*Sp[K-2]^3,Qpmap(K-1))
-------------------------------
K=2
0000
K=3
0000
K=4
0000
-------------------------------
Calculation and checking of the Bp[I], Bm[I], Cp[I], Cm[I]
-------------------------------
I=1
POLYPOLYPOLYPOLY
I=2
POLYPOLYPOLYPOLY
I=3
POLYPOLYPOLYPOLY
I=4
POLYPOLYPOLYPOLY
-------------------------------
8: Type of the Dm(I) and Dp(I)
-------------------------------
I=1
POLYPOLY
I=2
POLYPOLY
I=3
POLYPOLY
I=4
POLYPOLY
```

```
------------------------------
Plus Type

------------------------------
DEp2=ChCo2p[25]

------------------------------
DEp3=ChCo2p[19]

------------------------------
DFp2=ChCo1p[25]

------------------------------
DFp3=ChCo1p[19]

------------------------------
```

We give here the final output for the minus type map

```
------------------------------
Minus Type

------------------------------
DEm2=ChCo2m[25]

------------------------------
DEm3=ChCo2m[19]

------------------------------
DFm2=ChCo1m[25]

------------------------------
DFm3=ChCo1m[19]

------------------------------
```

E.3 Explicit presentation of the invariants a_3, a_2

We present the new invariants, generated as above, explicitly for the case $n = 4$ and $q = 3$ with quadratic form Q_s.

```
A43:=-x[1]^12x[2]^6 - x[1]^10x[2]^8 - x[1]^8x[2]^10 - x[1]^6x[2]^12 - x[1]^12x[2]^4x[3]^2
+ x[1]^10x[2]^6x[3]^2 + x[1]^8x[2]^8x[3]^2 + x[1]^6x[2]^10x[3]^2 - x[1]^4x[2]^12x[3]^2
- x[1]^12x[2]^2x[3]^4 + x[1]^10x[2]^4x[3]^4 + x[1]^4x[2]^10x[3]^4 - x[1]^2x[2]^12x[3]^4
- x[1]^12x[3]^6 + x[1]^10x[2]^2x[3]^6 - x[1]^6x[2]^6x[3]^6 + x[1]^2x[2]^10x[3]^6 - x[2]^12x[3]^6
- x[1]^10x[3]^8 + x[1]^8x[2]^2x[3]^8 + x[1]^2x[2]^8x[3]^8 - x[2]^10x[3]^8 - x[1]^8x[3]^10
+ x[1]^6x[2]^2x[3]^10 + x[1]^4x[2]^4x[3]^10 + x[1]^2x[2]^6x[3]^10 - x[2]^8x[3]^10
- x[1]^6x[3]^12 - x[1]^4x[2]^2x[3]^12 - x[1]^2x[2]^4x[3]^12 - x[2]^6x[3]^12
- x[1]^12x[2]^4x[4]^2 + x[1]^10x[2]^6x[4]^2 + x[1]^8x[2]^8x[4]^2 + x[1]^6x[2]^10x[4]^2
- x[1]^4x[2]^12x[4]^2 - x[1]^12x[2]^2x[3]^2x[4]^2 - x[1]^8x[2]^6x[3]^2x[4]^2
- x[1]^6x[2]^8x[3]^2x[4]^2 - x[1]^2x[2]^12x[3]^2x[4]^2 - x[1]^12x[3]^4x[4]^2
+ x[1]^8x[2]^4x[3]^4x[4]^2 + x[1]^4x[2]^8x[3]^4x[4]^ - x[2]^12x[3]^4x[4]^2 + x[1]^10x[3]^6x[4]^2
- x[1]^8x[2]^2x[3]^6x[4]^2 - x[1]^2x[2]^8x[3]^6x[4]^2 + x[2]^10x[3]^6x[4]^2 + x[1]^8x[3]^8x[4]^2
- x[1]^6x[2]^2x[3]^8x[4]^2 + x[1]^4x[2]^4x[3]^8x[4]^2 - x[1]^2x[2]^6x[3]^8x[4]^2
+ x[2]^8x[3]^8x[4]^2 + x[1]^6x[3]^10x[4]^2 + x[2]^6x[3]^10x[4]^2 - x[1]^4x[3]^12x[4]^2
- x[1]^2x[2]^2x[3]^12x[4]^2 - x[2]^4x[3]^12x[4]^2 - x[1]^12x[2]^2x[4]^4 + x[1]^10x[2]^4x[4]^4
+ x[1]^4x[2]^10x[4]^4 - x[1]^2x[2]^12x[4]^4 - x[1]^12x[3]^2x[4]^4 + x[1]^8x[2]^4x[3]^2x[4]^4
+ x[1]^4x[2]^8x[3]^2x[4]^4 - x[2]^12x[3]^2x[4]^4 + x[1]^10x[3]^4x[4]^4 + x[1]^8x[2]^2x[3]^4x[4]^4
- x[1]^6x[2]^4x[3]^4x[4]^4 - x[1]^4x[2]^6x[3]^4x[4]^4 + x[1]^2x[2]^8x[3]^4x[4]^4
+ x[2]^10x[3]^4x[4]^4 - x[1]^4x[2]^4x[3]^6x[4]^4 + x[1]^4x[2]^2x[3]^8x[4]^4
+ x[1]^2x[2]^4x[3]^8x[4]^4 + x[1]^4x[3]^10x[4]^4 + x[2]^4x[3]^10x[4]^4 - x[1]^2x[3]^12x[4]^4
- x[2]^2x[3]^12x[4]^4 - x[1]^12x[4]^6 + x[1]^10x[2]^2x[4]^6 - x[1]^6x[2]^6x[4]^6
+ x[1]^2x[2]^10x[4]^6 - x[2]^12x[4]^6 + x[1]^10x[3]^2x[4]^6 - x[1]^8x[2]^2x[3]^2x[4]^6
- x[1]^2x[2]^8x[3]^2x[4]^6 + x[2]^10x[3]^2x[4]^6 - x[1]^4x[2]^4x[3]^4x[4]^6
- x[1]^6x[3]^6x[4]^6 - x[2]^6x[3]^6x[4]^6 - x[1]^2x[2]^2x[3]^8x[4]^6 + x[1]^2x[3]^10x[4]^6
+ x[2]^2x[3]^10x[4]^6 - x[3]^12x[4]^6 - x[1]^10x[4]^8 + x[1]^8x[2]^2x[4]^8 + x[1]^2x[2]^8x[4]^8
- x[2]^10x[4]^8 + x[1]^8x[3]^2x[4]^8 - x[1]^6x[2]^2x[3]^2x[4]^8 + x[1]^4x[2]^4x[3]^2x[4]^8
- x[1]^2x[2]^6x[3]^2x[4]^8 + x[2]^8x[3]^2x[4]^8 + x[1]^4x[2]^2x[3]^4x[4]^8
+ x[1]^2x[2]^4x[3]^4x[4]^8 - x[1]^2x[2]^2x[3]^6x[4]^8 + x[1]^2x[3]^8x[4]^8 + x[2]^2x[3]^8x[4]^8
- x[3]^10x[4]^8 - x[1]^8x[4]^10 + x[1]^6x[2]^2x[4]^10 + x[1]^4x[2]^4x[4]^10 + x[1]^2x[2]^6x[4]^10
- x[2]^8x[4]^10 + x[1]^6x[3]^2x[4]^10 + x[2]^6x[3]^2x[4]^10 + x[1]^4x[3]^4x[4]^10
+ x[2]^4x[3]^4x[4]^10 + x[1]^2x[3]^6x[4]^10 + x[2]^2x[3]^6x[4]^10 - x[3]^8x[4]^10 - x[1]^6x[4]^12
- x[1]^4x[2]^2x[4]^12 - x[1]^2x[2]^4x[4]^12 - x[2]^6x[4]^12 - x[1]^4x[3]^2x[4]^12
- x[1]^2x[2]^2x[3]^2x[4]^12 - x[2]^4x[3]^2x[4]^12 - x[1]^2x[3]^4x[4]^12 - x[2]^2x[3]^4x[4]^12
```

```
- x[3]^6x[4]^12;
----------------------------
A42:= x[1]^12x[2]^8x[3]^4 + x[1]^10x[2]^10x[3]^4 + x[1]^8x[2]^12x[3]^4 + x[1]^12x[2]^6x[3]^6
- x[1]^10x[2]^8x[3]^6 - x[1]^8x[2]^10x[3]^6 + x[1]^6x[2]^12x[3]^6 + x[1]^12x[2]^4x[3]^8
- x[1]^10x[2]^6x[3]^8 - x[1]^6x[2]^10x[3]^8 + x[1]^4x[2]^12x[3]^8 + x[1]^10x[2]^4x[3]^10
- x[1]^8x[2]^6x[3]^10 - x[1]^6x[2]^8x[3]^10 + x[1]^4x[2]^10x[3]^10 + x[1]^8x[2]^4x[3]^12
+ x[1]^6x[2]^6x[3]^12 + x[1]^4x[2]^8x[3]^12 + x[1]^12x[2]^8x[3]^2x[4]^2
+ x[1]^10x[2]^10x[3]^2x[4]^2 + x[1]^8x[2]^12x[3]^2x[4]^2 - x[1]^12x[2]^6x[3]^4x[4]^2
+ x[1]^10x[2]^8x[3]^4x[4]^2 + x[1]^8x[2]^10x[3]^4x[4]^2 - x[1]^6x[2]^12x[3]^4x[4]^2
- x[1]^12x[2]^4x[3]^6x[4]^2 - x[1]^10x[2]^6x[3]^6x[4]^2 + x[1]^8x[2]^8x[3]^6x[4]^2
- x[1]^6x[2]^10x[3]^6x[4]^2 - x[1]^4x[2]^12x[3]^6x[4]^2 + x[1]^12x[2]^2x[3]^8x[4]^2
+ x[1]^10x[2]^4x[3]^8x[4]^2 + x[1]^8x[2]^6x[3]^8x[4]^2 + x[1]^6x[2]^8x[3]^8x[4]^2
+ x[1]^4x[2]^10x[3]^8x[4]^2 + x[1]^2x[2]^12x[3]^8x[4]^2 + x[1]^10x[2]^2x[3]^10x[4]^2
+ x[1]^8x[2]^4x[3]^10x[4]^2 - x[1]^6x[2]^6x[3]^10x[4]^2 + x[1]^4x[2]^8x[3]^10x[4]^2
+ x[1]^2x[2]^10x[3]^10x[4]^2 + x[1]^8x[2]^2x[3]^12x[4]^2 - x[1]^6x[2]^4x[3]^12x[4]^2
- x[1]^4x[2]^6x[3]^12x[4]^2 + x[1]^2x[2]^8x[3]^12x[4]^2 + x[1]^12x[2]^8x[4]^4
+ x[1]^10x[2]^10x[4]^4 + x[1]^8x[2]^12x[4]^4 - x[1]^12x[2]^6x[3]^2x[4]^4
+ x[1]^10x[2]^8x[3]^2x[4]^4 + x[1]^8x[2]^10x[3]^2x[4]^4 - x[1]^6x[2]^12x[3]^2x[4]^4
+ x[1]^10x[2]^6x[3]^4x[4]^4 + x[1]^8x[2]^8x[3]^4x[4]^4 + x[1]^6x[2]^10x[3]^4x[4]^4
- x[1]^12x[2]^2x[3]^6x[4]^4 + x[1]^10x[2]^4x[3]^6x[4]^4 + x[1]^4x[2]^10x[3]^6x[4]^4
- x[1]^2x[2]^12x[3]^6x[4]^4 + x[1]^12x[3]^8x[4]^4 + x[1]^10x[2]^2x[3]^8x[4]^4
+ x[1]^8x[2]^4x[3]^8x[4]^4 + x[1]^4x[2]^8x[3]^8x[4]^4 + x[1]^2x[2]^10x[3]^8x[4]^4
+ x[2]^12x[3]^8x[4]^4 + x[1]^10x[3]^10x[4]^4 + x[1]^8x[2]^2x[3]^10x[4]^4
+ x[1]^6x[2]^4x[3]^10x[4]^4 + x[1]^4x[2]^6x[3]^10x[4]^4 + x[1]^2x[2]^8x[3]^10x[4]^4
+ x[2]^10x[3]^10x[4]^4 + x[1]^8x[3]^12x[4]^4 - x[1]^6x[2]^2x[3]^12x[4]^4
- x[1]^2x[2]^6x[3]^12x[4]^4 + x[2]^8x[3]^12x[4]^4 + x[1]^12x[2]^6x[4]^6 - x[1]^10x[2]^8x[4]^6
- x[1]^8x[2]^10x[4]^6 + x[1]^6x[2]^12x[4]^6 - x[1]^12x[2]^4x[3]^2x[4]^6
- x[1]^10x[2]^6x[3]^2x[4]^6 + x[1]^8x[2]^8x[3]^2x[4]^6 - x[1]^6x[2]^10x[3]^2x[4]^6
- x[1]^4x[2]^12x[3]^2x[4]^6 - x[1]^12x[2]^2x[3]^4x[4]^6 + x[1]^10x[2]^4x[3]^4x[4]^6
+ x[1]^4x[2]^10x[3]^4x[4]^6 - x[1]^2x[2]^12x[3]^4x[4]^6 + x[1]^12x[3]^6x[4]^6
- x[1]^10x[2]^2x[3]^6x[4]^6 - x[1]^2x[2]^10x[3]^6x[4]^6 + x[2]^12x[3]^6x[4]^6
- x[1]^10x[3]^8x[4]^6 + x[1]^8x[2]^2x[3]^8x[4]^6 + x[1]^2x[2]^8x[3]^8x[4]^6 - x[2]^10x[3]^8x[4]^6
- x[1]^8x[3]^10x[4]^6 - x[1]^6x[2]^2x[3]^10x[4]^6 + x[1]^4x[2]^4x[3]^10x[4]^6
- x[1]^2x[2]^6x[3]^10x[4]^6 - x[2]^8x[3]^10x[4]^6 + x[1]^6x[3]^12x[4]^6
- x[1]^4x[2]^2x[3]^12x[4]^6 - x[1]^2x[2]^4x[3]^12x[4]^6 + x[2]^6x[3]^12x[4]^6
+ x[1]^12x[2]^4x[4]^8 - x[1]^10x[2]^6x[4]^8 - x[1]^6x[2]^10x[4]^8 + x[1]^4x[2]^12x[4]^8
+ x[1]^12x[2]^2x[3]^2x[4]^8 + x[1]^10x[2]^4x[3]^2x[4]^8 + x[1]^8x[2]^6x[3]^2x[4]^8
+ x[1]^6x[2]^8x[3]^2x[4]^8 + x[1]^4x[2]^10x[3]^2x[4]^8 + x[1]^2x[2]^12x[3]^2x[4]^8
```

```
+ x[1]^12x[3]^4x[4]^8 + x[1]^10x[2]^2x[3]^4x[4]^8 + x[1]^8x[2]^4x[3]^4x[4]^8
+ x[1]^4x[2]^8x[3]^4x[4]^8 + x[1]^2x[2]^10x[3]^4x[4]^8 + x[2]^12x[3]^4x[4]^8
- x[1]^10x[3]^6x[4]^8 + x[1]^8x[2]^2x[3]^6x[4]^8 + x[1]^2x[2]^8x[3]^6x[4]^8 - x[2]^10x[3]^6x[4]^8
+ x[1]^6x[2]^2x[3]^8x[4]^8 + x[1]^4x[2]^4x[3]^8x[4]^8 + x[1]^2x[2]^6x[3]^8x[4]^8
- x[1]^6x[3]^10x[4]^8 + x[1]^4x[2]^2x[3]^10x[4]^8 + x[1]^2x[2]^4x[3]^10x[4]^8
- x[2]^6x[3]^10x[4]^8 + x[1]^4x[3]^12x[4]^8 + x[1]^2x[2]^2x[3]^12x[4]^8 + x[2]^4x[3]^12x[4]^8
+ x[1]^10x[2]^4x[4]^10 - x[1]^8x[2]^6x[4]^10 - x[1]^6x[2]^8x[4]^10 + x[1]^4x[2]^10x[4]^10
+ x[1]^10x[2]^2x[3]^2x[4]^10 + x[1]^8x[2]^4x[3]^2x[4]^10 - x[1]^6x[2]^6x[3]^2x[4]^10
+ x[1]^4x[2]^8x[3]^2x[4]^10 + x[1]^2x[2]^10x[3]^2x[4]^10 + x[1]^10x[3]^4x[4]^10
+ x[1]^8x[2]^2x[3]^4x[4]^10 + x[1]^6x[2]^4x[3]^4x[4]^10 + x[1]^4x[2]^6x[3]^4x[4]^10
+ x[1]^2x[2]^8x[3]^4x[4]^10 + x[2]^10x[3]^4x[4]^10 - x[1]^8x[3]^6x[4]^10
- x[1]^6x[2]^2x[3]^6x[4]^10 + x[1]^4x[2]^4x[3]^6x[4]^10 - x[1]^2x[2]^6x[3]^6x[4]^10
- x[2]^8x[3]^6x[4]^10 - x[1]^6x[3]^8x[4]^10 + x[1]^4x[2]^2x[3]^8x[4]^10
+ x[1]^2x[2]^4x[3]^8x[4]^10 - x[2]^6x[3]^8x[4]^10 + x[1]^4x[3]^10x[4]^10
+ x[1]^2x[2]^2x[3]^10x[4]^10 + x[2]^4x[3]^10x[4]^10 + x[1]^8x[2]^4x[4]^12 + x[1]^6x[2]^6x[4]^12
+ x[1]^4x[2]^8x[4]^12 + x[1]^8x[2]^2x[3]^2x[4]^12 - x[1]^6x[2]^4x[3]^2x[4]^12
- x[1]^4x[2]^6x[3]^2x[4]^12 + x[1]^2x[2]^8x[3]^2x[4]^12 + x[1]^8x[3]^4x[4]^12
- x[1]^6x[2]^2x[3]^4x[4]^12 - x[1]^2x[2]^6x[3]^4x[4]^12 + x[2]^8x[3]^4x[4]^12
+ x[1]^6x[3]^6x[4]^12 - x[1]^4x[2]^2x[3]^6x[4]^12 - x[1]^2x[2]^4x[3]^6x[4]^12
+ x[2]^6x[3]^6x[4]^12 + x[1]^4x[3]^8x[4]^12 + x[1]^2x[2]^2x[3]^8x[4]^12 + x[2]^4x[3]^8x[4]^12;
-------------------------------
```

Appendix F

Investigations in the ring

$R_0 = \mathbb{F}_q\langle \xi_0, \xi_1, \xi_1, d_3, d_2 \rangle$

F.1 Code to calculate expressions in the ring $R_0 = \mathbb{F}_q\langle \xi_0, \xi_1, \xi_1, d_3, d_2 \rangle$

We present code for calculating given expressions in terms of the polynomials ξ_0, ξ_1, ξ_1, d_3 and d_2. The expressions are input as Pol following the input of the ring generators and d_1.

Output from the code defining ξ_3 and d_1 in terms with of the generators is given in Appendix F.2.

```
N:=4; MEMORY.N:=N; P:=3; MEMORY.P:=P; D:=1; Q:=P^D; MEMORY.Q:=Q;
I:=3; MEMORY.I:=I; Nm:=N-1;
Use RR::=Z/(P)[t,x[1..N],s[0..Nm],d[2..3]];RR;

-----------------------------------------------------------------
-- C calculates Dickson invariant C(N,I)from Dickson matrix DM(N)
-- CF is the list of coefficients of powers of t in the determinant of DM in descending order

Define C(N,I) Q:=MEMORY.Q; DM:=NewMat(N+1,N+1);
    For A:=1 To N+1 Do For B:=1 To N Do
        DM[A,B]:=x[B]^(Q^(A-1))
    EndFor; DM[A,N+1]:=t^(Q^(A-1)) EndFor; -- Println DM;
    CF:=Coefficients(Det(DM),t); C:=CF[Q^N-Q^I+1]/CF[1];
Return C EndDefine;
-----------------------------------------------------------------
-- The procedure Xi(I) generates the Xi(j)s from Xi(0):=x[1]^2+....+ x[n]^2
```

```
Define Xi(I) Q:=MEMORY.Q; N:=MEMORY.N; Xi:=0;
    For A:=1 To N Do Xi:=Xi+x[A]^(Q^I+1) EndFor;
Return Xi EndDefine;
-----------------------------------------------------------------
-- D43 and D42  having been generated previously are given explictly

D43:=x[1]^18 - x[1]^16x[2]^2 - x[1]^14x[2]^4 - x[1]^12x[2]^6 + x[1]^10x[2]^8 + x[1]^8x[2]^10
- x[1]^6x[2]^12 - x[1]^4x[2]^14 - x[1]^2x[2]^16 + x[2]^18 - x[1]^16x[3]^2 - x[1]^12x[2]^4x[3]^2
+ x[1]^10x[2]^6x[3]^2 + x[1]^6x[2]^10x[3]^2 - x[1]^4x[2]^12x[3]^2 - x[2]^16x[3]^2
- x[1]^14x[3]^4 - x[1]^12x[2]^2x[3]^4 + x[1]^10x[2]^4x[3]^4 + x[1]^4x[2]^10x[3]^4
- x[1]^2x[2]^12x[3]^4 - x[2]^14x[3]^4 - x[1]^12x[3]^6 + x[1]^10x[2]^2x[3]^6
- x[1]^6x[2]^6x[3]^6 + x[1]^2x[2]^10x[3]^6 - x[2]^12x[3]^6 + x[1]^10x[3]^8 + x[2]^10x[3]^8
+ x[1]^8x[3]^10 + x[1]^6x[2]^2x[3]^10 + x[1]^4x[2]^4x[3]^10 + x[1]^2x[2]^6x[3]^10
+ x[2]^8x[3]^10 - x[1]^6x[3]^12 - x[1]^4x[2]^2x[3]^12 - x[1]^2x[2]^4x[3]^12 - x[2]^6x[3]^12
- x[1]^4x[3]^14 - x[2]^4x[3]^14 - x[1]^2x[3]^16 - x[2]^2x[3]^16 + x[3]^18 - x[1]^16x[4]^2
- x[1]^12x[2]^4x[4]^2 + x[1]^10x[2]^6x[4]^2 + x[1]^6x[2]^10x[4]^2 - x[1]^4x[2]^12x[4]^2
- x[2]^16x[4]^2 - x[1]^12x[2]^2x[3]^2x[4]^2 + x[1]^10x[2]^4x[3]^2x[4]^2
+ x[1]^4x[2]^10x[3]^2x[4]^2 - x[1]^2x[2]^12x[3]^2x[4]^2 - x[1]^12x[3]^4x[4]^2
+ x[1]^10x[2]^2x[3]^4x[4]^2 - x[1]^6x[2]^6x[3]^4x[4]^2 + x[1]^2x[2]^10x[3]^4x[4]^2
- x[2]^12x[3]^4x[4]^2 + x[1]^10x[3]^6x[4]^2 - x[1]^6x[2]^4x[3]^6x[4]^2
- x[1]^4x[2]^6x[3]^6x[4]^2 + x[2]^10x[3]^6x[4]^2 + x[1]^6x[3]^10x[4]^2
+ x[1]^4x[2]^2x[3]^10x[4]^2 + x[1]^2x[2]^4x[3]^10x[4]^2 + x[2]^6x[3]^10x[4]^2
- x[1]^4x[3]^12x[4]^2 - x[1]^2x[2]^2x[3]^12x[4]^2 - x[2]^4x[3]^12x[4]^2 - x[3]^16x[4]^2
- x[1]^14x[4]^4 - x[1]^12x[2]^2x[4]^4 + x[1]^10x[2]^4x[4]^4 + x[1]^4x[2]^10x[4]^4
- x[1]^2x[2]^12x[4]^4 - x[2]^14x[4]^4 - x[1]^12x[3]^2x[4]^4 + x[1]^10x[2]^2x[3]^2x[4]^4
- x[1]^6x[2]^6x[3]^2x[4]^4 + x[1]^2x[2]^10x[3]^2x[4]^4 - x[2]^12x[3]^2x[4]^4
+ x[1]^10x[3]^4x[4]^4 - x[1]^6x[2]^4x[3]^4x[4]^4 - x[1]^4x[2]^6x[3]^4x[4]^4
+ x[2]^10x[3]^4x[4]^4 - x[1]^6x[2]^2x[3]^6x[4]^4 - x[1]^4x[2]^4x[3]^6x[4]^4
- x[1]^2x[2]^6x[3]^6x[4]^4 + x[1]^4x[3]^10x[4]^4 + x[1]^2x[2]^2x[3]^10x[4]^4
+ x[2]^4x[3]^10x[4]^4 - x[1]^2x[3]^12x[4]^4 - x[2]^2x[3]^12x[4]^4 - x[3]^14x[4]^4
- x[1]^12x[4]^6 + x[1]^10x[2]^2x[4]^6 - x[1]^6x[2]^6x[4]^6 + x[1]^2x[2]^10x[4]^6
- x[2]^12x[4]^6 + x[1]^10x[3]^2x[4]^6 - x[1]^6x[2]^4x[3]^2x[4]^6 - x[1]^4x[2]^6x[3]^2x[4]^6
+ x[2]^10x[3]^2x[4]^6 - x[1]^6x[2]^2x[3]^4x[4]^6 - x[1]^4x[2]^4x[3]^4x[4]^6
- x[1]^2x[2]^6x[3]^4x[4]^6 - x[1]^6x[3]^6x[4]^6 - x[1]^4x[2]^2x[3]^6x[4]^6
- x[1]^2x[2]^4x[3]^6x[4]^6 - x[2]^6x[3]^6x[4]^6 + x[1]^2x[3]^10x[4]^6 + x[2]^2x[3]^10x[4]^6
- x[3]^12x[4]^6 + x[1]^10x[4]^8 + x[2]^10x[4]^8 + x[3]^10x[4]^8 + x[1]^8x[4]^10
+ x[1]^6x[2]^2x[4]^10 + x[1]^4x[2]^4x[4]^10 + x[1]^2x[2]^6x[4]^10 + x[2]^8x[4]^10
+ x[1]^6x[3]^2x[4]^10 + x[1]^4x[2]^2x[3]^2x[4]^10 + x[1]^2x[2]^4x[3]^2x[4]^10
```

```
+ x[2]^6x[3]^2x[4]^10 + x[1]^4x[3]^4x[4]^10 + x[1]^2x[2]^2x[3]^4x[4]^10 + x[2]^4x[3]^4x[4]^10
+ x[1]^2x[3]^6x[4]^10 + x[2]^2x[3]^6x[4]^10 + x[3]^8x[4]^10 - x[1]^6x[4]^12
- x[1]^4x[2]^2x[4]^12 - x[1]^2x[2]^4x[4]^12 - x[2]^6x[4]^12 - x[1]^4x[3]^2x[4]^12
- x[1]^2x[2]^2x[3]^2x[4]^12 - x[2]^4x[3]^2x[4]^12 - x[1]^2x[3]^4x[4]^12 - x[2]^2x[3]^4x[4]^12
- x[3]^6x[4]^12 - x[1]^4x[4]^14 - x[2]^4x[4]^14 - x[3]^4x[4]^14 - x[1]^2x[4]^16 - x[2]^2x[4]^16
- x[3]^2x[4]^16 + x[4]^18;

D42:=-x[1]^24 - x[1]^22x[2]^2 + x[1]^20x[2]^4 - x[1]^14x[2]^10 - x[1]^10x[2]^14 + x[1]^4x[2]^20
- x[1]^2x[2]^22 - x[2]^24 - x[1]^22x[3]^2 + x[1]^18x[2]^4x[3]^2 - x[1]^12x[2]^10x[3]^2
- x[1]^10x[2]^12x[3]^2 + x[1]^4x[2]^18x[3]^2 - x[2]^22x[3]^2 + x[1]^20x[3]^4
+ x[1]^18x[2]^2x[3]^4 + x[1]^10x[2]^10x[3]^4 + x[1]^2x[2]^18x[3]^4 + x[2]^20x[3]^4
+ x[1]^12x[2]^6x[3]^6 + x[1]^6x[2]^12x[3]^6 - x[1]^14x[3]^10 - x[1]^12x[2]^2x[3]^10
+ x[1]^10x[2]^4x[3]^10 + x[1]^4x[2]^10x[3]^10 - x[1]^2x[2]^12x[3]^10 - x[2]^14x[3]^10
- x[1]^10x[2]^2x[3]^12 + x[1]^6x[2]^6x[3]^12 - x[1]^2x[2]^10x[3]^12 - x[1]^10x[3]^14
- x[2]^10x[3]^14 + x[1]^4x[2]^2x[3]^18 + x[1]^2x[2]^4x[3]^18 + x[1]^4x[3]^20 + x[2]^4x[3]^20
- x[1]^2x[3]^22 - x[2]^2x[3]^22 - x[3]^24 - x[1]^22x[4]^2 + x[1]^18x[2]^4x[4]^2
- x[1]^12x[2]^10x[4]^2 - x[1]^10x[2]^12x[4]^2 + x[1]^4x[2]^18x[4]^2 - x[2]^22x[4]^2
+ x[1]^18x[2]^2x[3]^2x[4]^2 + x[1]^10x[2]^10x[3]^2x[4]^2 + x[1]^2x[2]^18x[3]^2x[4]^2
+ x[1]^18x[3]^4x[4]^2 + x[1]^12x[2]^6x[3]^4x[4]^2 + x[1]^6x[2]^12x[3]^4x[4]^2
+ x[2]^18x[3]^4x[4]^2 + x[1]^12x[2]^4x[3]^6x[4]^2 - x[1]^10x[2]^6x[3]^6x[4]^2
- x[1]^6x[2]^10x[3]^6x[4]^2 + x[1]^4x[2]^12x[3]^6x[4]^2 - x[1]^12x[3]^10x[4]^2
+ x[1]^10x[2]^2x[3]^10x[4]^2 - x[1]^6x[2]^6x[3]^10x[4]^2 + x[1]^2x[2]^10x[3]^10x[4]^2
- x[2]^12x[3]^10x[4]^2 - x[1]^10x[3]^12x[4]^2 + x[1]^6x[2]^4x[3]^12x[4]^2
+ x[1]^4x[2]^6x[3]^12x[4]^2 - x[2]^10x[3]^12x[4]^2 + x[1]^4x[3]^18x[4]^2
+ x[1]^2x[2]^2x[3]^18x[4]^2 + x[2]^4x[3]^18x[4]^2 - x[3]^22x[4]^2 + x[1]^20x[4]^4
+ x[1]^18x[2]^2x[4]^4 + x[1]^10x[2]^10x[4]^4 + x[1]^2x[2]^18x[4]^4 + x[2]^20x[4]^4
+ x[1]^18x[3]^2x[4]^4 + x[1]^12x[2]^6x[3]^2x[4]^4 + x[1]^6x[2]^12x[3]^2x[4]^4
+ x[2]^18x[3]^2x[4]^4 + x[1]^12x[2]^4x[3]^4x[4]^4 - x[1]^10x[2]^6x[3]^4x[4]^4
- x[1]^6x[2]^10x[3]^4x[4]^4 + x[1]^4x[2]^12x[3]^4x[4]^4 + x[1]^12x[2]^2x[3]^6x[4]^4
- x[1]^10x[2]^4x[3]^6x[4]^4 - x[1]^4x[2]^10x[3]^6x[4]^4 + x[1]^2x[2]^12x[3]^6x[4]^4
+ x[1]^10x[3]^10x[4]^4 - x[1]^6x[2]^4x[3]^10x[4]^4 - x[1]^4x[2]^6x[3]^10x[4]^4
+ x[2]^10x[3]^10x[4]^4 + x[1]^6x[2]^2x[3]^12x[4]^4 + x[1]^4x[2]^4x[3]^12x[4]^4
+ x[1]^2x[2]^6x[3]^12x[4]^4 + x[1]^2x[3]^18x[4]^4 + x[2]^2x[3]^18x[4]^4 + x[3]^20x[4]^4
+ x[1]^12x[2]^6x[4]^6 + x[1]^6x[2]^12x[4]^6 + x[1]^12x[2]^4x[3]^2x[4]^6
- x[1]^10x[2]^6x[3]^2x[4]^6 - x[1]^6x[2]^10x[3]^2x[4]^6 + x[1]^4x[2]^12x[3]^2x[4]^6
+ x[1]^12x[2]^2x[3]^4x[4]^6 - x[1]^10x[2]^4x[3]^4x[4]^6 - x[1]^4x[2]^10x[3]^4x[4]^6
+ x[1]^2x[2]^12x[3]^4x[4]^6 + x[1]^12x[3]^6x[4]^6 - x[1]^10x[2]^2x[3]^6x[4]^6
+ x[1]^6x[2]^6x[3]^6x[4]^6 - x[1]^2x[2]^10x[3]^6x[4]^6 + x[2]^12x[3]^6x[4]^6
```

```
- x[1]^6x[2]^2x[3]^10x[4]^6 - x[1]^4x[2]^4x[3]^10x[4]^6 - x[1]^2x[2]^6x[3]^10x[4]^6
+ x[1]^6x[3]^12x[4]^6 + x[1]^4x[2]^2x[3]^12x[4]^6 + x[1]^2x[2]^4x[3]^12x[4]^6
+ x[2]^6x[3]^12x[4]^6 - x[1]^14x[4]^10 - x[1]^12x[2]^2x[4]^10 + x[1]^10x[2]^4x[4]^10
+ x[1]^4x[2]^10x[4]^10 - x[1]^2x[2]^12x[4]^10 - x[2]^14x[4]^10 - x[1]^12x[3]^2x[4]^10
+ x[1]^10x[2]^2x[3]^2x[4]^10 - x[1]^6x[2]^6x[3]^2x[4]^10 + x[1]^2x[2]^10x[3]^2x[4]^10
- x[2]^12x[3]^2x[4]^10 + x[1]^10x[3]^4x[4]^10 - x[1]^6x[2]^4x[3]^4x[4]^10
- x[1]^4x[2]^6x[3]^4x[4]^10 + x[2]^10x[3]^4x[4]^10 - x[1]^6x[2]^2x[3]^6x[4]^10
- x[1]^4x[2]^4x[3]^6x[4]^10 - x[1]^2x[2]^6x[3]^6x[4]^10 + x[1]^4x[3]^10x[4]^10
+ x[1]^2x[2]^2x[3]^10x[4]^10 + x[2]^4x[3]^10x[4]^10 - x[1]^2x[3]^12x[4]^10
- x[2]^2x[3]^12x[4]^10 - x[3]^14x[4]^10 - x[1]^10x[2]^2x[4]^12 + x[1]^6x[2]^6x[4]^12
- x[1]^2x[2]^10x[4]^12 - x[1]^10x[3]^2x[4]^12 + x[1]^6x[2]^4x[3]^2x[4]^12
+ x[1]^4x[2]^6x[3]^2x[4]^12 - x[2]^10x[3]^2x[4]^12 + x[1]^6x[2]^2x[3]^4x[4]^12
+ x[1]^4x[2]^4x[3]^4x[4]^12 + x[1]^2x[2]^6x[3]^4x[4]^12 + x[1]^6x[3]^6x[4]^12
+ x[1]^4x[2]^2x[3]^6x[4]^12 + x[1]^2x[2]^4x[3]^6x[4]^12 + x[2]^6x[3]^6x[4]^12
- x[1]^2x[3]^10x[4]^12 - x[2]^2x[3]^10x[4]^12 - x[1]^10x[4]^14 - x[2]^10x[4]^14
- x[3]^10x[4]^14 + x[1]^4x[2]^2x[4]^18 + x[1]^2x[2]^4x[4]^18 + x[1]^4x[3]^2x[4]^18
+ x[1]^2x[2]^2x[3]^2x[4]^18 + x[2]^4x[3]^2x[4]^18 + x[1]^2x[3]^4x[4]^18 + x[2]^2x[3]^4x[4]^18
+ x[1]^4x[4]^20 + x[2]^4x[4]^20 + x[3]^4x[4]^20 - x[1]^2x[4]^22 - x[2]^2x[4]^22
- x[3]^2x[4]^22 - x[4]^24;

MEMORY.D43:=D43; MEMORY.D42:=D42;
-----------------------------------------------------------------

--To find if Xi(3) in Fq[xi0,xi1,xi2,d43,d42]
Pol:=Xi(3); DX:=Deg(Pol);
-- NExpr is the number of possible polynomials Exp(A,B,C,D,E) of degree equal to deg(xi3)
NExpr:=0;
AH:=Div(DX,24);
For A:=AH To 0 Step -1 Do BH:=Div((DX-A*24),18); For B:=BH To 0 Step -1 Do
    CH:=Div((DX-A*24-B*18),10);
    For C:=CH To 0 Step -1 Do DH:=Div((DX-A*24-B*18-C*10),4);
        For D:=DH To 0 Step -1 Do E:=(DX-A*24-B*18-C*10-D*4)/2; NExpr:=NExpr+1;
EndFor EndFor EndFor EndFor;
PrintLn 'The number of possible forms Exp(A,B,C,D,E) of degree equal to deg(xi3) is ',NExpr;
MEMORY.NExpr:=NExpr;

-- EDM is the matrix giving on each row a set of possible degrees of the generating polynomials
EDM:=NewMat(NExpr,5); Count:=1;
```

```
For A:=AH To 0 Step -1 Do BH:=Div((DX-A*24),18);
    For B:=BH To 0 Step -1 Do CH:=Div((DX-A*24-B*18),10);
        For C:=CH To 0 Step -1 Do DH:=Div((DX-A*24-B*18-C*10),4);
         For D:=DH To 0 Step -1 Do E:=(DX-A*24-B*18-C*10-D*4)/2;
                EDM[Count,1]:=A; EDM[Count,2]:=B; EDM[Count,3]:=C;
                EDM[Count,4]:=D; EDM[Count,5]:=E; Count:=Count+1;
EndFor EndFor EndFor EndFor;

-----------------------------------------------------------------

-- NTerms is the maximum number of terms in the homogeneous polynomials of degree equal to that
-- of Deg(Pol) that have all even indices and that are distinct
-- (terms with permuted indices are not counted as distinct)
NTerms:=0; For Dx1:=DX To Div(DX,N) Step -2 Do
    DR1:=DX-Dx1; Deg1:=Min([DR1,Dx1]);
    For Dx2:=Deg1 To Div(DR1,N-1) Step -2 Do
        DR2:=DX -Dx1-Dx2; Deg2:=Min([DR2,Dx2]);
        For Dx3:=Deg2 To Div(DR2,N-2) Step -2 Do NTerms:=NTerms+1;
EndFor EndFor EndFor;
PrintLn("The number of 'distinct' terms is ", NTerms);
MEMORY.NTerms:=NTerms;

DEGS:=NewMat(NTerms,N); DegC:=1;
For Dx1:=DX To Div(DX,N) Step -2 Do
    DR1:=DX-Dx1; Deg1:=Min([DR1,Dx1]);
    For Dx2:=Deg1 To Div(DR1,N-1) Step -2 Do
        DR2:=DX-Dx1-Dx2; Deg2:=Min([DR2,Dx2]);
        For Dx3:=Deg2 To Div(DR2,N-2) Step -2 Do Dx4:=DX-Dx1-Dx2-Dx3;
            DEGS[DegC,1]:=Dx1; DEGS[DegC,2]:=Dx2; DEGS[DegC,3]:=Dx3; DEGS[DegC,4]:=Dx4;
DegC:=DegC+1;
EndFor EndFor EndFor;
-------------------------------------------------------------------

-- ExpCo extracts the coefficients of terms in a given polynomial that have constituent
-- indices even (In this work all terms with constituent indices odd have coefficient 0)
-- We call these the usable coefficients
-- Also to reduce size the  'symmetrical' coefficients have been removed
```

```
Define ExpCo(Ply) N:=MEMORY.N; Q:=MEMORY.Q; P:=MEMORY.P; Deg:=Deg(Ply);
  NTerms:=MEMORY.NTerms; Count:=1; CoeffList:=NewList(NTerms);
  For Dx1:=Deg To Div(Deg,N) Step -2 Do DR1:=Deg-Dx1; Deg1:=Min([DR1,Dx1]);
    For Dx2:=Deg1 To Div(DR1,N-1) Step -2 Do DR2:=Deg-Dx1-Dx2; Deg2:=Min([DR2,Dx2]);
      For Dx3:=Deg2 To Div(DR2,N-2) Step -2 Do Dx4:=Deg-Dx1-Dx2-Dx3;
      CoeffList[Count]:=Mod((CoeffOfTerm(x[1]^Dx1*x[2]^Dx2*x[3]^Dx3*x[4]^Dx4,Ply)*(1%P)),P);
      Count:=Count+1;
  EndFor EndFor EndFor;
Return CoeffList EndDefine;
-----------------------------------------------------------------

-- CoMat is a matrix whose rows contain the "usable" coefficient of the
-- Exp(A,B,C,D,E) polynomials in the generators of the ring,R0, and of Xi(3)

CoMat:=NewMat(NExpr+1,NTerms);

Define Exp(A,B,C,D,E)
D43:=MEMORY.D43; D42:=MEMORY.D42; Exp:=D42^A*D43^B*Xi(2)^C*Xi(1)^D*Xi(0)^E;
Return Exp EndDefine;

For I:=1 To NExpr Do CoMat[I]:=ExpCo(Exp(EDM[I,1],EDM[I,2],EDM[I,3],EDM[I,4],EDM[I,5])) EndFor;
CoMat[NExpr+1]:=ExpCo(Xi(3));

--PrintLn("The matrix of the usable coefficients is ",CoMat);
-----------------------------------------------------------------

-- The following prcedure reduces the transpose of the coefficient matrix to reduced row echelon
-- form giving the last column of the transposed matrix as the solution vector.
-- RowDiv returns the matrix M with Ath row scaled to give M[A,A]=1 if M[A,A]<>0
-- Needs the XInv procedure to find multiplicative inverse of M[A,A]

Define XInv(I)
    For A:=1 To MEMORY.Q-1 Do B:=I*A;
        If Mod(B,MEMORY.P)=1 Then XInv:=A EndIf; EndFor;
Return XInv; EndDefine;

Define RowDiv(M,A) Rows:=Len(M); Cols:=Len(M[1]); Pivot:=M[A,A];
    If Pivot<>0 Then PDiv:=XInv(Pivot); --PrintLn(PDiv);
```

```
        For B:=1 To Cols Do M[A,B]:=Mod(M[A,B]*PDiv,MEMORY.P) EndFor; EndIf;
Return M EndDefine;
-----------------------------------------------------------------------

-- For each row, check whether M[A,A]<>0 and if so do Row Div and subtract M[B,A]*Row A from
-- Row B row. If M[A,A]=0 then find a M[B,A]<>0 if possible and exchange rows then do above.
Define ColClear(M,A) Rows:=Len(M); Cols:=Len(M[1]);
    If M[A,A]=0 Then Temp:=M[A]; For B:=A+1 To Rows Do
         If M[B,A]<>0 Then M[A]:=M[B]; M[B]:=Temp; Break
    EndIf EndFor EndIf;
    If M[A,A]<>0 Then M:=RowDiv(M,A);
    For B:=1 To Rows Do If B<>A Then Scal:=M[B,A];
       For B1:=1 To Cols Do M[B,B1]:=Mod(M[B,B1]-M[A,B1]*Scal,MEMORY.P) EndFor;
    EndIf EndFor EndIf;
Return M EndDefine;

-- RowRed reduces an augmented matrix to reduced row echelon form
Define RowRed(M) Rows:=Len(M); Cols:=Len(M[1]); Reps:=Min(Cols-1,Rows);
    For A:=1 To Reps Do M:=ColClear(M,A) EndFor;
Return M EndDefine;
-----------------------------------------------------------------------

-- Implementing the row reduce procedure to find the given form in terms of the generators
SM:=RowRed(Transposed(CoMat)); Cols:=Len(SM[1]); Cols1:=Cols-1;
SMT:=Transposed(SM); Sol:=Submat(SMT,[Cols],1..Cols1);Sol1:=Sol[1];
PrintLn("Solutions for n=",N," and q=",Q," are ",Sol1);
PolExp:=0;
For J:=1 To NExpr Do
    Pl:=Sol1[J]*d[2]^EDM[J,1]*d[3]^EDM[J,2]*s[2]^EDM[J,3]*s[1]^EDM[J,4]*s[0]^EDM[J,5];
PolExp:=PolExp+Pl EndFor;
If PolExp= Subst(Pol,[[s[0],Xi(0)],[s[1],Xi(1)],[s[2],Xi(2)],[d[2],D42],[d[3],D43]])
 Then PrintLn 'Pol=',Pol Else PrintLn FALSE EndIf;;
```

F.2 Output for code in Appendix F.1

Below we give the output of the above code with Pol:=Xi(3) giving in particular ξ_3 as a polynomial in $\xi_0, \xi_1, \xi_1, d_3, d_2$.

```
Z/(3)[t,x[1..4],s[0..3],d[2..3]]
--------------------------------
The number of number of possible polynomials Exp(A,B,C,D,E) of degree equal to
deg(xi3) is 22


--------------------------------
The number of 'distinct' terms is 47


--------------------------------
Solutions for n=4 and q=3 are
[2, 0, 2, 2, 0, 1, 0, 1, 0, 0, 2, 0, 2, 0, 2, 0, 1, 0, 2, 0, 0, 0]


--------------------------------
Pol=-s[0]^8s[1]^3 + s[0]^4s[1]^5 - s[0]^7s[1]s[2] - s[1]^7 - s[0]^3s[1]^3s[2] + s[0]^5d[3]
                          + s[0]^2s[1]s[2]^2 - s[0]s[1]^2d[3] - s[1]d[2] - s[2]d[3]
--------------------------------
```

The code above calculates d_1, as defined in the statement of Conjecture 4.1, as a polynomial in the generators of the ring R_0 with Pol:=Xi(3); replaced by Pol:=D41. The explicit expression for D41 is included in the code as given in the output in Appendix B.5.

The polynomial for d_1 in terms of $\xi_0, \xi_1, \xi_1, d_3, d_2$ is then given below.

```
--------------------------------
Pol=s[0]^11s[1] + s[0]^7s[1]^3 - s[0]^3s[1]^5 + s[0]^6s[1]s[2] + s[0]^2s[1]^3s[2] - s[0]^4d[3]
            - s[0]s[1]s[2]^2 + s[1]^2d[3]
--------------------------------
```

F.3 The kernel of the map Q_4^+

We give here the code used to calculate the generators of the kernel of the map Q_4^+ presented in Definition 7.1 together with the output from the code. We have omitted the explicit expressions for d_3 and d_2 as D43 and D42 to save space. These can be copied from the code in Appendix F.1.

Thus we have the relation on the ring R_0.

```
N:=4; MEMORY.N:=N; P:=3; MEMORY.P:=P; D:=1; Q:=P^D; MEMORY.Q:=Q;
Use S::=Z/(3)[x[1..4]];
R0::=Z/(3)[s[0..2],d[2..3]];

-- The procedure Xi(I) generates the Xi(j)s from Xi(0):=x[1]^2+....+ x[n]^2

Define Xi(I)
    Q:=MEMORY.Q; N:=MEMORY.N;
    Xi:=0; For A:=1 To N Do Xi:=Xi+x[A]^(Q^I+1) EndFor;
    Return Xi
EndDefine;
-----------------------------------------------------------
D43:=; --Copy expression for D43 from previous section

D42:=; --Copy expression for D42 from previous section

Qmap:=Alg.Map('R0','S',[Xi(0),Xi(1),Xi(2),D42,D43]);
Use R0;
QmapKer:=Gens(Alg.Ker(Theta));
QmapKer;
Eval(QmapKer,[0]);

[-s[0]^11s[1]^2 - s[0]^7s[1]^4 + s[0]^10s[2] + s[0]^3s[1]^6 - s[0]^6s[1]^2s[2] - s[0]^2s[1]^4s[2]
+ s[0]^4s[1]d[3] + s[0]s[1]^2s[2]^2 - s[0]^3d[2] + s[1]^3d[3] + s[2]^3]

--------------------------------
[s[1]^3d[3] + s[2]^3]

--------------------------------
```

References

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Perseus, Oxford, 1969.

[2] Tom Apostol M, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1976.

[3] D. J. Benson, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series, vol. 190, Cambridge University Press, Cambridge, 1993.

[4] Peter J. Cameron, *Introduction to algebra*, Oxford Science Publications, Oxford University Press, Oxford, 1998.

[5] ———, *Projective and polar spaces*, QMW Maths Notes, vol. 13, Queen Mary and Westfield College School of Mathematical Sciences, London.

[6] D. Carlisle and P. H. Kropholler, *Rational invariants of certain orthogonal and unitary groups*, Bull. London Math. Soc. **24** (1992), no. 1, 57–60.

[7] Li Chiang and Yu Ch'ing Hung, *The invariants of orthogonal group actions*, Bull. Austral. Math. Soc. **48** (1993), no. 2, 313–319.

[8] Huah Chu, *Polynomial invariants of four-dimensional orthogonal groups*, Comm. Algebra **29** (2001), no. 3, 1153–1164.

[9] Leonard Eugene Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. **12** (1911), no. 1, 75–98.

[10] David S Dummit and Richard M Foote, *Abstract Algebra*, 2nd ed., Wiley, New York, 1999.

[11] William Fulton, *Young tableaux*, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997. With applications to representation theory and geometry.

[12] J. W. P. Hirschfeld, *Projective geometries over finite fields*, 2nd ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.

[13] P. H. Kropholler, S. Mohseni Rajaei, and J. Segal, *Invariant rings of orthogonal groups over* $\mathbb{F}_2$, Glasg. Math. J. **47** (2005), no. 1, 7–54.

[14] Rudolf Lidl and Harald Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. With a foreword by P. M. Cohn.

[15] Peter J. Olver, *Classical invariant theory*, London Mathematical Society Student Texts, vol. 44, Cambridge University Press, Cambridge, 1999.

[16] O. Timothy O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[17] Mara D. Neusel and Larry Smith, *Invariant theory of finite groups*, Mathematical Surveys and Monographs, vol. 94, American Mathematical Society, Providence, RI, 2002.

[18] Larry Smith and R Strong E., *On the Invariant theory of finite groups: Orbit Polynomials and Splitting Principles*, Journal of Algebra **110** (1987), 134-157.

[19] Larry Smith, *The ring of invariants of* $\mathrm{O}(3, \mathbf{F}_q)$, Finite Fields Appl. **5** (1999), no. 1, 96–101.

[20] ———, *Polynomial invariants of finite groups. A survey of recent developments*, Bull. Amer. Math. Soc. (N.S.) **34** (1997), no. 3, 211–250.

[21] ———, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995.

[22] Ian Stewart, *Galois Theory*, 3rd ed., Chapman & Hall/CRC Mathematics, Chapman & Hall/CRC, Boca Raton, FL, 2004.

[23] Clarence Wilkerson, *A primer on the Dickson invariants*, Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982) **19** (1983), 421–434.

[24] R. M. W. Wood, *Differential operators and the Steenrod algebra*, Proc. London Math. Soc. (3) **75** (1997), no. 1, 194–220.