JOURNAL OF COMMUTATIVE ALGEBRA
Volume 2, Number 4, Winter 2010

NON-VANISHING FORMS IN PROJECTIVE SPACE OVER FINITE FIELDS

SAMUEL LUNDQVIST

ABSTRACT. We consider a subset of projective space over a finite field and give bounds on the minimal degree of a non-vanishing form with respect to this subset. We also give an algorithm to compute a non-vanishing form.

1. Introduction. Let $\mathbf{X} = \{p_1, \dots, p_m\}$ be a set of points in $\mathbf{P}^n(\mathbf{k})$, where $\mathbf{k}$ is a field. We say that a form f in $\mathbf{k}[x_0, \dots, x_n]$ is non-vanishing with respect to $\mathbf{X}$ if $f(p_i) \neq 0$ for all i. When $\mathbf{k}$ is an infinite field, there is an infinite number of linear forms which are non-vanishing on $\mathbf{X}$. This is not always the case when $\mathbf{k}$ is a finite field. Consider $\mathbf{X} = \{(1:0), (0:1), (1:1)\} \subseteq \mathbf{P}^1(\mathbf{F}_2)$, where $\mathbf{F}_2$ denotes the finite field with two elements. There are three linear forms in $\mathbf{F}_2[x_0, x_1]$: x_0, x_1 and $x_0 + x_1$. We have

$$x_0((0:1)) = x_1((1:0)) = (x_0 + x_1)((1:1)) = 0.$$

Thus, there is no linear non-vanishing form with respect to $\mathbf{X}$.

When $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{k})$, let $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \geq 1$ denote the least degree of a non-vanishing form f with respect to $\mathbf{X}$. Denote by $\mathbf{F}_q$ the field with q elements. In this paper, we will give bounds on $\operatorname{Deg}\operatorname{Nz}(\mathbf{X})$ when $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$ and an algorithm to compute a non-vanishing form.

In the language of commutative algebra, a form f in $\mathbf{k}[x_0, \dots, x_n]$ is non-vanishing with respect to a set of projective points $\mathbf{X}$ if and only if $[f]$ is a non-zero divisor in the quotient ring $\mathbf{k}[x_0, \dots, x_n]/I(\mathbf{X})$, where $I(\mathbf{X})$ is the vanishing ideal with respect to $\mathbf{X}$ and $[f]$ denotes the equivalence class of f in $\mathbf{k}[x_0, \dots, x_n]/I(\mathbf{X})$. Hence, $\operatorname{Deg}\operatorname{Nz}(\mathbf{X})$ is the least degree of a non-zero divisor in $\mathbf{k}[x_0, \dots, x_n]/I(\mathbf{X})$.

In Proposition 3.2 in [**2**], Kreuzer shows that when $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$ and $|\mathbf{X}| \leq q$, then $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = 1$ by using that an element $[f] \in$

Received by the editors on September 15, 2009, and in revised form on April 6, 2010.

DOI:10.1216/JCA-2010-2-4-437

$\mathbf{F}_q[x_0,\dots,x_n]/I(\mathbf{X})$ is a non-zero divisor if f does not belong to the union of the associated primes of $I(\mathbf{X})$. The same result using the same method is given independently in [**4**]. In that paper, linear non-zero divisors play an important role for computing varieties over one-dimensional graded rings. In this paper we obtain the result as a special case of Theorem 4.3.

The existence of a non-zero divisor can also be stated in terms of the union of finite subspaces of $\mathbf{k}[x_0,\dots,x_n]$ as follows. Let $\mathbf{X} = \{p_1,\dots,p_m\}$, and let $I(p_i)$ be the set of all homogeneous polynomials vanishing on p_i. Let $A = \cup_i I(p_i)$, and let d be the least positive degree such that $\mathbf{k}[x_0,\dots,x_n]_d$ is not contained in A. Then $d = \operatorname{Deg}\operatorname{Nz}(\mathbf{X})$.

Finally, if $\mathbf{X}$ is the set of $\mathbf{F}_q$ rational points of a hypersurface, given by a form f in $\mathbf{F}_q[x_0,\dots,x_n]$, then $\operatorname{Deg}\operatorname{Nz}(\mathbf{X})$ is the least degree of a form g such that the variety determined by the ideal (f,g), has no $\mathbf{F}_q$ rational points.

2. Preliminaries. The results that we will present in this paper rely upon Warning's theorem (Satz 3 in [**5**]), which states that if the equation $f = 0$, where f in $\mathbf{F}_q[x_1,\dots,x_n]$ is an element of degree $d < n$, has a solution, then it has at least q^{n-d} solutions. We give the projective version of the result as a lemma.

Lemma 2.1. *Let f be a non-constant form in $\mathbf{F}_q[x_0,\dots,x_n]$ of degree $d < n+1$. Then there are at least $1 + q + \cdots + q^{n-d}$ solutions to $f = 0$ in $\mathbf{P}^n(\mathbf{F}_q)$.*

Proof. By Warning's theorem, there are at least q^{n-d+1} solutions in $\mathbf{F}_q^{n+1}$. Removing the trivial solution, we are left with at least $q^{n-d+1}-1$ zeroes. Thus, the number of projective solutions is at least $(q^{n-d+1}-1)/(q-1) = 1 + q + \cdots + q^{n-d}$. □

The requirement on d in Warning's theorem is sharp. Indeed, Lang (Theorem 1 in [**3**]) gives a construction of a form of degree $n+1$ in $\mathbf{F}_q[x_0,\dots,x_n]$ which is non-vanishing with respect to $\mathbf{P}^n(\mathbf{F}_q)$–it is the norm of the element $x_0e_0 + \cdots + x_ne_n$, where $\{e_0,\dots,e_n\}$ is a basis for an extension $\mathbf{F}_{q^{n+1}}$ of $\mathbf{F}_q$ of degree $n+1$. Recall that the norm of an

element α in $\mathbf{F}_{q^{n+1}}$ is defined as

$$\mathrm{Nm}\,(\alpha) = \alpha \cdot \mathrm{Fr}_q(\alpha) \cdot \mathrm{Fr}_q^2(\alpha) \cdots \mathrm{Fr}_q^n(\alpha),$$

where Fr_q is the Frobenius map

$$\mathrm{Fr}_q : \mathbf{F}_{q^{n+1}} \to \mathbf{F}_{q^{n+1}}, \alpha \longmapsto \alpha^q.$$

Example 2.2. Suppose that we want to find a quadratic non-vanishing form with respect to $\mathbf{P}^1(\mathbf{F}_2)$. Since $1 + y + y^2$ is irreducible over $\mathbf{F}_2[y]$, a basis for the extension field $\mathbf{F}_4$ of $\mathbf{F}_2$ is $\{1, y\}$. We get

$$\begin{aligned}
\mathrm{Nm}\,(x_0 + x_1 y) &= (x_0 + x_1 y) \cdot \mathrm{Fr}_2(x_0 + x_1 y) \\
&= (x_0 + x_1 y) \cdot (\mathrm{Fr}_2(x_0) + \mathrm{Fr}_2(x_1)\mathrm{Fr}_2(y)) \\
&= (x_0 + x_1 y) \cdot (x_0 + x_1(1 + y)) \\
&= (x_0 + x_1 y)(x_0 + x_1 + x_1 y) \\
&= x_0^2 + x_0 x_1 + x_1^2.
\end{aligned}$$

The following lemma gives us our first bound on the least degree of a non-vanishing form f with respect to $\mathbf{X}$.

Lemma 2.3. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$. *Then* $\mathrm{Deg}\,\mathrm{Nz}\,(X) \leq n + 1$.

Proof. This is just a restatement of Theorem 1 in [**3**]. □

Some words about the notation. By saying that a subset $\mathbf{Y}$ of $\mathbf{X}$ is isomorphic to $\mathbf{P}^d(\mathbf{F}_q)$, we will mean *linearly* isomorphic. Hence, when $\mathbf{X}$ contains an isomorphic copy of $\mathbf{P}^d(\mathbf{F}_q)$, we can choose coordinates so that $(0 : \cdots : 0 : a_0 : \cdots : a_d) \in \mathbf{X}$ for all $(a_0, \ldots, a_d) \in \mathbf{F}_q^{d+1} \setminus (0, \ldots, 0)$. Likewise, when we write $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q) \setminus \mathbf{Y}$, with $\mathbf{Y} \cong \mathbf{P}^d(\mathbf{F}_q)$, we mean that there is a linearly isomorphic copy of $\mathbf{P}^d(\mathbf{F}_q)$ which has empty intersection with $\mathbf{X}$. In this situation it is possible to choose coordinates such that $(0 : \cdots : 0 : a_0 : \cdots : a_d) \notin \mathbf{X}$ for all $(a_0, \ldots, a_d) \in \mathbf{F}_q^{d+1} \setminus (0, \ldots, 0)$.

3. Geometric descriptions. In this section we give bounds on $\operatorname{Deg}\operatorname{Nz}(\mathbf{X})$ in terms of the geometric structure of $\mathbf{X}$.

Lemma 3.1. *Let* $\mathbf{Y} \subseteq \mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$*, and suppose that* $\mathbf{Y} \cong \mathbf{P}^d(\mathbf{F}_q)$*. Then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \geq d+1$*.*

Proof. Choose coordinates such that

$$(0 : \cdots : 0 : a_0 : \cdots : a_d) \in \mathbf{X}$$

for all $(a_0, \ldots, a_d) \in \mathbf{F}_q^{d+1} \setminus (0, \ldots, 0)$. Now consider a form f of degree $i < d+1$ with respect to these coordinates. Let

$$g = f(0, \ldots, 0, y_0, \ldots, y_d).$$

If $g = 0$, then $f(p) = 0$ for any point p in $\mathbf{Y}$. Otherwise, g is a form of degree i. By Lemma 2.1 $g = 0$ has at least one solution in $\mathbf{Y}$. Thus, in both cases, there is a point $p \in \mathbf{X}$ such that $f(p) = 0$. Hence $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \geq d+1$. □

In the following example we consider a subset $\mathbf{X}$ of $\mathbf{P}^2(\mathbf{F}_3)$ for which it holds that $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = 2$ although no isomorphic copy of $\mathbf{P}^1(\mathbf{F}_3)$ is contained in $\mathbf{X}$. Thus, Lemma 3.1 is non-sharp.

Example 3.2. Let

$$\mathbf{X} = \{(1:0:0), (0:1:0), (0:0:1), (1:1:0), (0:1:2), (1:0:1)\} \subset \mathbf{P}^2(\mathbf{F}_3).$$

It is an easy exercise to show that $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = 2$. If there was an isomorphic copy $\mathbf{Y}$ of $\mathbf{P}^1(\mathbf{F}_3)$ contained in $\mathbf{X}$, then there would be a linear change y_0, y_1, y_2 of coordinates such that $\mathbf{Y}$ is the zero locus of the linear polynomial y_0. Thus, to show that there is no isomorphic copy of $\mathbf{P}^1(\mathbf{F}_3)$ in $\mathbf{X}$, it is enough to show that for an arbitrary linear form $f = a_0x_0 + a_1x_1 + a_2x_2$, there are at most three points from $\mathbf{X}$ in the zero locus $Z(f)$ of f. Clearly, if two of the a_i's are zero, then $|Z(f)| = 3$. If only one of the a_i's is zero, then $|Z(f)| \leq 3$. For the remaining values of $(a_0 : a_1 : a_2)$ we have $|Z(x_0 + x_1 + x_2)| = 1$, $|Z(x_0 + x_1 + 2x_2)| = 1$ and $|Z(x_0 + 2x_1 + 2x_2)| = 3$.

To get a sharp version of Lemma 3.1, we have to put some extra requirements on the set $\mathbf{X}$. We need two lemmas before we can prove the sharp version in Proposition 3.6.

Lemma 3.3. *Let* $\mathbf{X} \subset \mathbf{P}^n(\mathbf{F}_q)$*, and suppose that* $(1:0\cdots:0) \notin \mathbf{X}$*. Let* π *be the projection from* $\mathbf{X}$ *to* $\mathbf{P}^{n-1}(\mathbf{F}_q)$ *defined by sending* $(a_0 : \cdots : a_n)$ *to* $(a_1 : \cdots : a_n)$*. Then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq \operatorname{Deg}\operatorname{Nz}(\pi(\mathbf{X}))$*.*

Proof. Since $(1 : 0 : \cdots : 0) \notin \mathbf{X}$, the projection is well defined. Let $f \in \mathbf{F}_q[x_1, \ldots, x_n]$ be any non-vanishing form on $\pi(\mathbf{X})$. Then the embedding of f into $\mathbf{F}_q[x_0, \ldots, x_n]$ gives a non-vanishing form with respect to $\mathbf{X}$. Hence $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq \operatorname{Deg}\operatorname{Nz}(\pi(\mathbf{X}))$. □

Remark 3.4. When $\mathbf{X} \subset \mathbf{P}^n(\mathbf{F}_q)$, i.e., there exists a point $p \in \mathbf{P}^n(\mathbf{F}_q) \setminus \mathbf{X}$, it is always possible to choose coordinates such that $p = (1 : 0 : \cdots : 0)$, and hence, define a projection from $\mathbf{X}$ to $\mathbf{P}^{n-1}(\mathbf{F}_q)$ by omitting the first coordinate.

Lemma 3.5. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$*, and suppose that there is a series of linear projections* $\mathbf{X} \mapsto \mathbf{X}^{(n-1)} \subseteq \mathbf{P}^{n-1}(\mathbf{F}_q), \mathbf{X}^{(n-1)} \mapsto \mathbf{X}^{(n-2)} \subseteq \mathbf{P}^{n-2}(\mathbf{F}_q), \ldots, \mathbf{X}^{(i+1)} \mapsto \mathbf{X}^{(i)} \subseteq \mathbf{P}^{i}(\mathbf{F}_q)$*, all defined by omitting the first coordinate after a suitable linear change of coordinates. Suppose further that* $\mathbf{X}^{(i)} \cong \mathbf{P}^d(\mathbf{F}_q)$*. Then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq d + 1$*.*

Proof. From successive use of Lemma 3.3, we obtain that $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq \operatorname{Deg}\operatorname{Nz}(\mathbf{X}^{(n-1)}) \leq \cdots \leq \operatorname{Deg}\operatorname{Nz}(\mathbf{X}^{(i)})$. We have $\operatorname{Deg}\operatorname{Nz}(\mathbf{P}^d(\mathbf{X})) = d+1$, so the lemma follows by repeating the embedding argument from Lemma 3.3. □

We now combine Lemma 3.1 and Lemma 3.5.

Proposition 3.6. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$*, and let* d *be the greatest integer for which there exists a* $\mathbf{Y} \subseteq \mathbf{X}$*, with* $\mathbf{Y} \cong \mathbf{P}^d(\mathbf{F}_q)$*. Suppose that there is a series of linear projections* $\mathbf{X} \mapsto \mathbf{X}^{(n-1)} \subseteq \mathbf{P}^{n-1}(\mathbf{F}_q), \mathbf{X}^{(n-1)} \mapsto \mathbf{X}^{(n-2)} \subseteq \mathbf{P}^{n-2}(\mathbf{F}_q), \ldots, \mathbf{X}^{(d+1)} \mapsto \mathbf{X}^{(d)} \cong \mathbf{Y}$ *all defined by omitting the first coordinate after a suitable linear change of coordinates. Then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = d + 1$*.*

Proof. By Lemma 3.1, $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \geq d+1$, and by Lemma 3.5, $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq d+1$. □

We end the chapter by giving a "cutting out" description of $\operatorname{Deg}\operatorname{Nz}(\mathbf{X})$.

Lemma 3.7. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q) \setminus \mathbf{Y}$, *where* $\mathbf{Y} \cong \mathbf{P}^d(\mathbf{X})$. *Then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq n-d$.

Proof. Choose coordinates such that

$$(0 : \cdots : 0 : a_0 : \cdots : a_d) \notin \mathbf{X}$$

for all $(a_0, \ldots, a_d) \in \mathbf{F}_q^{d+1} \setminus (0, \ldots, 0)$.

With respect to these coordinates, the map $\mathbf{X} \to \mathbf{P}^{n-d-1}(\mathbf{F}_q)$, $(a_0 : \cdots : a_n) \mapsto (a_0 : \cdots : a_{n-d-1})$ is well defined. By Lemma 2.3, there is a non-vanishing form in $\mathbf{F}_q[x_0, \ldots, x_{n-d-1}]$ of degree $n-d$. This form is naturally embedded into $\mathbf{F}_q[x_0, \ldots, x_n]$ and is non-vanishing on $\mathbf{X}$. □

4. Bounds on a non-vanishing form in terms of the number of elements.

Lemma 4.1. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$, *and let* d *be the least integer such that* $|\mathbf{X}| \leq q + \cdots + q^d$. *Then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq d$.

Proof. If $d > n$, then $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq d$ by Lemma 2.3. Suppose instead that $d \leq n$. We claim that it is possible to construct a series of linear projections $\mathbf{X} \mapsto \mathbf{X}^{(n-1)} \subseteq \mathbf{P}^{n-1}(\mathbf{F}_q), \mathbf{X}^{(n-1)} \mapsto \mathbf{X}^{(n-2)} \subseteq \mathbf{P}^{n-2}(\mathbf{F}_q), \ldots, \mathbf{X}^{(d)} \mapsto \mathbf{X}^{(d-1)} \subseteq \mathbf{P}^{d-1}(\mathbf{F}_q)$, all defined by omitting the first coordinate after a suitable linear change of coordinates. Thus, after proving the claim, the lemma follows from Lemma 3.5.

Since $|\mathbf{X}| < |\mathbf{P}^n(\mathbf{F}_q)|$ it follows from Remark 3.4 that it is possible to define a projection $\mathbf{X} \to \mathbf{X}^{(n-1)}$. If $d > n-1$, (e.g. $d = n$), then we are done. Else, we have $|\mathbf{X}^{(n-1)}| < |\mathbf{P}^{n-1}(\mathbf{F}_q)|$, and we can repeat the argument to finally obtain $\mathbf{X}^{(d-1)}$, which proves the claim. □

The upper bound is sharp in the sense that for any n and any d, there is a set $\mathbf{X}$ where d is the least integer such that $|\mathbf{X}| \leq q + \cdots + q^d$ and

$\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = d$. Indeed, let $\mathbf{X}$ be the image of any linear embedding of $\mathbf{P}^{d-1}(\mathbf{F}_q)$ into $\mathbf{P}^n(\mathbf{F}_q)$. Then we can apply Proposition 3.6 with $\mathbf{Y} = \mathbf{P}^{d-1}(\mathbf{F}_q)$, so it follows that $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = d$. Finally, d is easily verified to be the least integer such that $|\mathbf{X}| \leq q + \cdots + q^d$.

Lemma 4.2. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$. *If* $q^{n-d+2} + \cdots + q^n < |\mathbf{X}|$, *then* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \geq d$.

Proof. We can suppose that $d \geq 2$. Let f be a form of degree $d-1$. By Lemma 2.1, the number of projective solutions is at least $1 + q + \cdots + q^{n-d+1}$. It follows that there are at most $|\mathbf{P}^n(\mathbf{F}_q)| - (1 + q + \cdots + q^{n-d+1}) = q^{n-d+2} + \cdots + q^n$ points where f is non-vanishing. By assumption, $q^{n-d+2} + \cdots + q^n < |\mathbf{X}|$. Thus, there is a point $p \in \mathbf{X}$ such that $f(p) = 0$. Hence $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) > d-1$. □

The bound in Lemma 4.2 is also sharp in the same sense as described above. To see this, consider the set $\mathbf{X} = \mathbf{P}^n(\mathbf{F}_q) \setminus \mathbf{Y}$, where $\mathbf{Y}$ is any isomorphic copy of $\mathbf{P}^{n-d}(\mathbf{F}_q)$. By Lemma 3.7, we have $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq d$. But $|\mathbf{X}| = q^{n-d+1} + \cdots + q^n$, so $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \geq d$ by Lemma 4.1. Hence $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}) = d$.

We can state the following theorem.

Theorem 4.3. *Let* $\mathbf{X} \subseteq \mathbf{P}^n(\mathbf{F}_q)$. *If* $|\mathbf{X}| \leq q^n$, *let* $d_1 = 1$. *Otherwise, let* d_1 *be the greatest integer such that* $q^{n-d_1+2} + \cdots + q^n < |\mathbf{X}|$. *Let* d_2 *be the least integer such that* $|\mathbf{X}| \leq q + \cdots + q^{d_2}$. *Then*

$$d_1 \leq \operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq d_2.$$

The bounds are sharp in the sense that, for any n *and any* d, *there is a set* $\mathbf{X}_1$ *such that* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}_1)$ *assumes the lower bound, and a set* $\mathbf{X}_2$ *such that* $\operatorname{Deg}\operatorname{Nz}(\mathbf{X}_2)$ *assumes the upper bound.*

Proof. The first part of the theorem follows from Lemma 4.1 and Lemma 4.2. The second part follows from the remarks after Lemma 4.1 and Lemma 4.2. □

When $|\mathbf{X}| \leq q$, then $d_1 = d_2 = 1$, and we obtain Kreuzer's Proposition 3.2 [**2**] as a special case of Theorem 4.3.

5. An algorithm to compute a non-vanishing form. To find $\operatorname{Deg}\operatorname{Nz}(\mathbf{X})$ is by no means an easy computational task, so in order to get a fast method, we should not require that the degree of the returned form is minimal. The algorithm that we present below use the ideas of Lemma 4.1 and the degree of the returned form is bounded by d, where d is the least integer such that $|\mathbf{X}| \leq q + \cdots + q^d$.

Algorithm 5.1.

1. If $|\mathbf{X}| = |\mathbf{P}^n(\mathbf{F}_q)|$, return the norm form.

2. Else, there is a point $p \in \mathbf{P}^n(\mathbf{F}_q) \setminus \mathbf{X}$. Change coordinates so that $p = (0 : \cdots : 0 : 1)$. Project $\mathbf{X}$ to $\mathbf{X}' \subseteq \mathbf{P}^{n-1}(\mathbf{F}_q)$ by omitting the last coordinate. Let f be a form returned after performing step 1 with $n = n - 1$ and $\mathbf{X} = \mathbf{X}'$. Return f with respect to the original coordinates.

Note that to actually construct a non-vanishing form, we have to compute a norm form. Thus, our method relies on finding an irreducible over $\mathbf{F}_q[y]$. We refer the reader to [**1**], where algorithms to construct irreducibles are discussed.

Example 5.3. Consider $\mathbf{P}^3(\mathbf{F}_2)$ and the point set $\mathbf{X} = \{(1:1:1:0), (0:0:0:1), (1:0:0:0), (0:1:0:0), (0:0:1:0), (1:1:1:1)\}$ with respect to some coordinates x_0, x_1, x_2, x_3. We have $2^2 + 2 = 6$ and, hence, $1 \leq \operatorname{Deg}\operatorname{Nz}(\mathbf{X}) \leq 2$ by Theorem 4.3.

We will now perform Algorithm 5.1 on $\mathbf{X}$. Pick the point $(0:0:1:1) \notin \mathbf{X}$. With respect to the linear change of coordinates $y_0 = x_0$, $y_1 = x_1$, $y_2 = x_2 + x_3$ and $y_3 = x_3$, this point reads $(0:0:0:1)$. Thus, with respect to the coordinates y_0, y_1, y_2, y_3, we get $\mathbf{X} = \{(1:1:1:0), (0:0:1:1), (1:0:0:0), (0:1:0:0), (0:0:1:0), (1:1:0:1)\}$ and $(0:0:0:1) \notin \mathbf{X}$.

We project down to $\mathbf{P}^2(\mathbf{F}_2)$ and get the points $\pi(\mathbf{X}) = \{(1:1:1), (0:0:1), (1:0:0), (0:1:0), (1:1:0)\}$. Notice that $\pi(0:0:1:1) = \pi(0:0:1:0)$. Now we are looking for a non-vanishing form with respect to these five points in $\mathbf{P}^2(\mathbf{F}_2)$. We notice that the point $p' = (1:0:1)$ is missing from $\pi(\mathbf{X})$, so we consider the linear change of coordinates $z_0 = y_0 + y_2, z_1 = y_1, z_2 = y_2$ for which

$p' = (0 : 0 : 1)$. Then we get $\pi(\mathbf{X}) = \{(0 : 1 : 1), (1 : 0 : 1), (1 : 0 : 0), (0 : 1 : 0), (1 : 1 : 0)\}$ with respect to these coordinates. We project down to $\mathbf{P}^1(\mathbf{F}_2)$ to get the points $\{(0 : 1), (1 : 0), (1 : 1)\}$. From Example 2.2 we know that $z_0^2 + z_1^2 + z_0 z_1$ is non-vanishing. Hence $(y_0 + y_2)^2 + (y_0 + y_2)y_1 + y_1^2$ is non-vanishing on $\pi(\mathbf{X})$, and we get the following quadratic form which is non-vanishing on $\mathbf{X}$:

$$(x_0 + x_2 + x_3)^2 + (x_0 + x_2 + x_3)x_1 + x_1^2.$$

The non-vanishing form constructed by the algorithm in Example 5.2 is two, and is in fact equal to $\operatorname{Deg} \operatorname{Nz}(\mathbf{X})$. We can verify this by showing that there is an embedding of $\mathbf{P}^1(\mathbf{F}_2)$ in $\mathbf{X}$, since it then follows by Lemma 3.1 that $\operatorname{Deg} \operatorname{Nz}(\mathbf{X}) \geq 2$. Indeed, $\{(1 : 1 : 1 : 0), (0 : 0 : 0 : 1), (1 : 1 : 1 : 1)\} \cong \mathbf{P}^1(\mathbf{F}_2)$, which can be seen by changing coordinates to $x_0 + x_2, x_1 + x_2, x_2, x_3$.

Acknowledgments. The author would like to thank Torsten Ekedahl and one anonymous referee for providing useful suggestions and comments on the paper.

REFERENCES

1. L. Adleman and H. Lenstra, Jr., *Finding irreducible polynomials over finite fields*, STOC 1986, 350–355.

2. M. Kreuzer, *Computing Hilbert-Kunz functions of* 1*-dimensional graded rings*, Univ. Iagellonicae Acta Math. **45** (2007), 81–95.

3. S. Lang, *On quasi algebraic closure*, Ann. Math. **2** (1952), 373–390.

4. S. Lundqvist, *Multiplication matrices and ideals of projective dimension zero*, submitted.

5. E. Warning, *Bemerkung zur vorstehenden Arbeit von Herr Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 76–83.

Department of Mathematics, Stockholm University, SE-106 91 Stockholm, Sweden
Email address: samuel@math.su.se