Distribution of Inverses in Polynomial Rings

William D. Banks
Department of Mathematics, University of Missouri
Columbia, MO 65211, USA
bbanks@math.missouri.edu

and

Igor E. Shparlinski*
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract

Let $\mathbb{F}_p$ be the finite field with p elements, and let $F(X) \in \mathbb{F}_p[X]$ be a square-free polynomial. We show that in the ring $\mathcal{R} = \mathbb{F}_p[X]/F(X)$, the inverses of polynomials of small height are uniformly distributed. We also show that for any set $\mathcal{L} \subset \mathcal{R}$ of very small cardinality, for almost all $G \in \mathcal{R}$ the set of inverses $\{(G+f)^{-1} \mid f \in \mathcal{L}\}$ are uniformly distributed. These questions are motivated by applications to the NTRU cryptosystem.

*Corresponding author

1 Introduction

Let $p \geq 3$ be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements, which we represent by the set $\{0, \pm 1, \ldots, \pm(p-1)/2\}$.

Let $F(X) \in \mathbb{F}_p[X]$ be a fixed square-free polynomial of degree n.

Denote by $\mathcal{R}$ the polynomial ring $\mathbb{F}_p[X]/F(X)$. For any integer h in the range $0 \leq h \leq (p-1)/2$, let $\mathcal{R}(h)$ be the subset of $\mathcal{R}$ consisting of polynomials of the form

$$f(X) = f_0 + f_1 X + \ldots + f_{n-1} X^{n-1}, \qquad |f_\nu| \leq h, \qquad \nu = 0, \ldots, n-1.$$

For a given set $\mathcal{L} \subseteq \mathcal{R}$ and a polynomial $G \in \mathcal{R}$, we denote by $\mathcal{L}_G$ the set of "shifted" polynomials $\{G + f \mid f \in \mathcal{L}\}$.

For an arbitrary set $\mathcal{S} \subset \mathcal{R}$, we denote by $\mathcal{S}^*$ the subset of invertible polynomials in $\mathcal{S}$. In particular, $\mathcal{R}^*$, $\mathcal{R}(h)^*$ and $\mathcal{L}_G^*$ denotes the set of invertible polynomials in $\mathcal{R}$, $\mathcal{R}(h)$ and $\mathcal{L}_G$, respectively.

For a polynomial $f \in \mathcal{R}^*$, we denote by f^* its inverse in the ring $\mathcal{R}$, that is, f^* is the unique polynomial of degree at most $n-1$ such that $f(X)f^*(X) \equiv 1 \pmod{F(X)}$.

Recall that the cardinality of $\mathcal{R}^*$ is given by an analogue of the *Euler function*

$$|\mathcal{R}^*| = p^n \prod_{j=1}^{r} (1 - p^{-n_j}), \tag{1}$$

where $n_1, \ldots, n_r$ are the degrees of the $r \geq 1$ irreducible divisors of $F(X)$. In the special case $F(X) = X^n - 1$, more explicit expressions for n_j, $j = 1, \ldots, r$ (hence also for $|\mathcal{R}^*|$) are given in [6]; see also Section 6.5 of [1] and Section 7.5 of [5].

In this paper, we show that the inverses of polynomials in $\mathcal{R}(h)^*$ are uniformly distributed provided that $h \geq p^{1/2+\varepsilon}$. We also show that for almost all $G \in \mathcal{R}$, the inverses of polynomials in $\mathcal{L}_G^*$ are uniformly distributed, even for sets $\mathcal{L}$ of very small cardinality. These questions are motivated by applications to the recently discovered *NTRU cryptosystem* [2], whose public keys are related to inverses of polynomials from certain very special sets. In particular, it is important to show that these inverses look and behave like "random" polynomials from $\mathcal{R}$, since the message concealing properties of NTRU rely on this assumption. Unfortunately, the sets of polynomials

involved in NTRU seem to be too "thin" to be covered by the techniques presented here. Nevertheless, we hope that our results may give some insight into this problem. Moreover, the original scheme of NTRU can easily be modified to work with sets of polynomials for which our results do apply in a direct way. We remark that the aforementioned property of NTRU polynomials has never been doubted in practice, but obtaining rigorous theoretical results remains a very challenging problem.

Our main tools are bounds of character sums in the ring $\mathcal{R}$. We reduce the problem of estimating these sums to bounds for Kloosterman sums [3] and for more general sums with rational functions over finite fields [4].

Acknowledgement. We thank Jeff Hoffstein, Dan Lieman and Joe Silverman for attracting our interest in this problem and for many fruitful discussions.

Work supported in part, for W. B. by NSF grant DMS-0070628 and for I. S. by ARC grant A69700294.

2 Character Sums

Let $F(X) = F_1(X) \dots F_r(X)$ be the complete factorization of $F(X)$ into irreducible factors. Since $F(X)$ is square-free, all of these factors are pairwise distinct.

Recall that $\mathbb{F}_p[X]/G(X) \cong \mathbb{F}_{p^m}$ for any irreducible polynomial $G(X) \in \mathbb{F}_p[X]$ of degree $\deg G = m$. For each $j = 1, \dots, r$, we fix a root α_j of $F_j(X)$, and denote

$$\mathbb{K}_j = \mathbb{F}_{p^{n_j}} = \mathbb{F}_p(\alpha_j) \cong \mathbb{F}_p[X]/F_j(X), \tag{2}$$

where $n_j = \deg F_j$. For each j, let

$$\mathrm{Tr}_j(z) = \sum_{k=0}^{n_j-1} z^{p^k}$$

be the trace of $z \in \mathbb{K}_j$ to $\mathbb{F}_p$.

For each F_j, there are at most $(2h+1)^{n-1}$ polynomials $f \in \mathcal{R}$ which are divisible by F_j (indeed, given the $n-1$ highest coefficients of f, the constant term is uniquely determined since $F_j | f$). Consequently, we obtain that

$$(2h+1)^n - n(2h+1)^{n-1} \le |\mathcal{R}(h)^*| \le (2h+1)^n. \tag{3}$$

We also denote by $\mathcal{A}$ the direct product of fields

$$\mathcal{A} = \mathbb{K}_1 \times \ldots \times \mathbb{K}_r.$$

Then we have natural isomorphisms

$$\mathcal{R} \cong \mathbb{K}_1 \times \ldots \times \mathbb{K}_r = \mathcal{A}, \qquad \mathcal{R}^* \cong \mathbb{K}_1^* \times \ldots \times \mathbb{K}_r^* = \mathcal{A}^*, \tag{4}$$

given by the map that sends $f \in \mathcal{R}$ to $\mathbf{a}_f = (f(\alpha_1), \ldots, f(\alpha_r)) \in \mathcal{A}$. In particular, the relation (1) follows immediately from (4).

Given a vector $\mathbf{a} = (a_1, \ldots, a_r) \in \mathcal{A}$, we define the character $\chi_{\mathbf{a}}$ of $\mathcal{R}$ by

$$\chi_{\mathbf{a}}(f) = \prod_{j=1}^{r} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j f\left(\alpha_j\right)\right)\right), \qquad f \in \mathcal{R},$$

where

$$\mathbf{e}(z) = \exp(2\pi i z/p).$$

It is easy to see that $\{\chi_{\mathbf{a}} \,|\, \mathbf{a} \in \mathcal{A}\}$ is the complete group of additive characters of $\mathcal{R}$. In particular, for any polynomial $f \in \mathcal{R}$, we have

$$\sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(f) = \begin{cases} 0 & \text{if } f \neq 0, \\ p^n & \text{if } f = 0. \end{cases} \tag{5}$$

Our main results rely on upper bounds for the character sums

$$S_{\mathbf{a}}(h) = \sum_{f \in \mathcal{R}(h)^*} \chi_{\mathbf{a}}(f^*) \qquad \text{and} \qquad W_{\mathbf{a}}(\mathcal{L}) = \sum_{G \in \mathcal{R}} \left| \sum_{f \in \mathcal{L}_G^*} \chi_{\mathbf{a}}(f^*) \right|.$$

To estimate these sums we need the identity (see Exercise 11.a in Chapter 3 of [7])

$$\sum_{c=0}^{p-1} \mathbf{e}(cu) = \begin{cases} 0 & \text{if } u \not\equiv 0 \pmod{p}, \\ p & \text{if } u \equiv 0 \pmod{p}, \end{cases} \tag{6}$$

which holds for any integer u, and the inequality (see Exercise 11.b in Chapter 3 of [7])

$$\sum_{c=0}^{p-1} \left| \sum_{u=-h}^{h} \mathbf{e}\left(cu\right) \right| \leq p(1 + \ln p), \tag{7}$$

which holds for any integer h in the range $0 \leq h \leq (p-1)/2$.

We also need the following simple statement.

Lemma 1 *For any vector* $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_p^n$*, there exists a unique vector* $\mathbf{b} = (b_1, \ldots, b_r) \in \mathcal{A}$ *such that*

$$\sum_{\nu=0}^{n-1} c_\nu f_\nu = \sum_{j=1}^{r} \mathrm{Tr}_j\left(b_j f\left(\alpha_j\right)\right)$$

for all polynomials

$$f(X) = f_0 + f_1 X + \ldots + f_{n-1} X^{n-1} \in \mathcal{R}.$$

Proof. Because the trace is a linear mapping, the identity of the theorem is equivalent to the system of equations

$$\sum_{j=1}^{r} \mathrm{Tr}_j\left(b_j \alpha_j^\nu\right) = c_\nu, \qquad \nu = 0, \ldots, n-1.$$

Thus for every vector $\mathbf{b} = (b_1, \ldots, b_r) \in \mathcal{A}$, there exists a unique vector $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_p^n$. Because $F(X)$ is square-free the elements

$$\alpha_j^{p^k}, \qquad k = 0, \ldots, n_j - 1, \quad j = 1, \ldots, r,$$

are pairwise distinct. From the property of the Vandermonde matrix we see that for every $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_p^n$, there is at most one vector $\mathbf{b} = (b_1, \ldots, b_r) \in \mathcal{A}$. Taking into account the fact that $|\mathcal{A}| = p^n = |\mathbb{F}_p^n|$, we obtain the desired statement. □

Now we are prepared to bound the sums $S_{\mathbf{a}}(h)$ and $W_{\mathbf{a}}(\mathcal{L})$.

Lemma 2 *Let* $\mathbf{a} = (a_1, \ldots, a_r) \in \mathcal{A}$ *and let* $\mathcal{J} \subseteq \{1, \ldots, r\}$ *be the set of* j *with* $a_j \neq 0$*. Then for any integer* h*,* $0 \leq h \leq (p-1)/2$ *the bound*

$$|S_{\mathbf{a}}(h)| \leq 2^{|\mathcal{J}|} p^{n/2} (1 + \ln p)^n \prod_{j \notin \mathcal{J}} p^{n_j/2}$$

holds.

Proof. From the identity (6) we derive

$$\begin{aligned} S_{\mathbf{a}}(h) &= \frac{1}{p^n} \sum_{f \in \mathcal{R}^*} \chi_{\mathbf{a}}(f^*) \sum_{c_0, \ldots, c_{n-1} \in \mathbb{F}_p} \sum_{u_0, \ldots, u_{n-1} = -h}^{h} \mathbf{e}\left(\sum_{\nu=0}^{n-1} c_\nu \left(f_\nu - u_\nu\right)\right) \\ &= \frac{1}{p^n} \sum_{c_0, \ldots, c_{n-1} \in \mathbb{F}_p} \sum_{u_0, \ldots, u_{n-1} = -h}^{h} \mathbf{e}\left(-\sum_{\nu=0}^{n-1} c_\nu u_\nu\right) \\ &\qquad \times \sum_{f \in \mathcal{R}^*} \chi_{\mathbf{a}}(f^*) \mathbf{e}\left(\sum_{\nu=0}^{n-1} c_\nu f_\nu\right) \end{aligned}$$

where $f(X) = f_0 + f_1X + \ldots + f_{n-1}X^{n-1}$. From Lemma 1 we see that for any vector $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_p^n$ there exist a vector $\mathbf{b} = (b_1, \ldots, b_r) \in \mathcal{A}$ such that

$$\begin{aligned}\sum_{f \in \mathcal{R}^*} \chi_{\mathbf{a}}(f^*)\mathbf{e}\left(\sum_{\nu=0}^{n-1} c_\nu f_\nu\right) &= \sum_{f \in \mathcal{R}^*} \chi_{\mathbf{a}}(f^*)\chi_{\mathbf{b}}(f) \\ &= \sum_{f \in \mathcal{R}^*} \prod_{j=1}^{r} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j f^*\left(\alpha_j\right) + b_j f\left(\alpha_j\right)\right)\right).\end{aligned}$$

From the isomorphism (4) it follows that as f runs over the set $\mathcal{R}^*$, the vector $\left(f\left(\alpha_1\right), \ldots, f\left(\alpha_r\right)\right)$ runs over $\mathbb{K}_1^* \times \ldots \times \mathbb{K}_r^*$. Since $f^*\left(\alpha_j\right) = \left(f\left(\alpha_j\right)\right)^{-1}$, $j = 1, \ldots, r$, we have

$$\begin{aligned}\sum_{f \in \mathcal{R}^*} \chi_{\mathbf{a}}(f^*)\mathbf{e}\left(\sum_{\nu=0}^{n-1} c_\nu f_\nu\right) &= \sum_{x_1 \in \mathbb{K}_1^*} \ldots \sum_{x_r \in \mathbb{K}_r^*} \prod_{j=1}^{r} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j x_j^{-1} + b_j x_j\right)\right) \\ &= \prod_{j=1}^{r} \sum_{x_j \in \mathbb{K}_j^*} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j x_j^{-1} + b_j x_j\right)\right).\end{aligned}$$

Sums with $j \notin \mathcal{J}$ we estimate trivially as p^{n_j}, and for sums with $j \in \mathcal{J}$ we use the Kloosterman bound (see Theorem 5.45 of [3])

$$\left|\sum_{x_j \in \mathbb{K}_j^*} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j x_j^{-1} + b_j x_j\right)\right)\right| \le 2p^{n_j/2}.$$

Thus

$$\left|\sum_{f \in \mathcal{R}^*} \chi_{\mathbf{a}}(f^*)\mathbf{e}\left(\sum_{\nu=0}^{n-1} c_\nu f_\nu\right)\right| \le 2^{|\mathcal{J}|} \prod_{j \notin \mathcal{J}} p^{n_j} \prod_{j \in \mathcal{J}} p^{n_j/2} = 2^{|\mathcal{J}|} p^{n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2}.$$

Applying the inequality (7), we obtain the desired result. □

Lemma 3 *Let $\mathbf{a} = (a_1, \ldots, a_r) \in \mathcal{A}$ and let $\mathcal{J} \subseteq \{1, \ldots, r\}$ be the set of j with $a_j \neq 0$. Then the bound*

$$W_{\mathbf{a}}(\mathcal{L}) \le 2n^{1/2} 3^{|\mathcal{J}|/2} p^n |\mathcal{L}|^{3/4} \prod_{j \notin \mathcal{J}} p^{n_j/4}$$

holds.

Proof. From the Cauchy inequality we derive

$$\begin{aligned} W_{\mathbf{a}}(\mathcal{L})^2 &\le p^n \sum_{G\in\mathcal{R}} \left| \sum_{f\in\mathcal{L}_G^*} \chi_{\mathbf{a}}(f^*) \right|^2 \\ &= p^n \sum_{G\in\mathcal{R}} \sum_{f_1,f_2\in\mathcal{L}_G^*} \chi_{\mathbf{a}}(f_1^* - f_2^*) \\ &\le p^n \left(p^n|\mathcal{L}| + \sum_{G\in\mathcal{R}} \sum_{\substack{f_1,f_2\in\mathcal{L}_G^* \\ f_1\ne f_2}} \chi_{\mathbf{a}}(f_1^* - f_2^*) \right) \\ &= p^n \left(p^n|\mathcal{L}| + \sum_{\substack{f_1,f_2\in\mathcal{L} \\ f_1\ne f_2}} \sum_{G\in\mathcal{R}}^* \chi_{\mathbf{a}}((G+f_1)^* - (G+f_2)^*) \right), \end{aligned}$$

where Σ^* means that the sum is taken over all polynomials $G \in \mathcal{R}$ for which both $G + f_1$ and $G + f_2$ are invertible. From the isomorphism (4) it follows that as G runs over this set, the vector $(G(\alpha_1), \ldots, G(\alpha_r))$ runs over the set $\mathcal{A}_{f_1,f_2}$ of elements $(x_1, \ldots, x_r)$ in $\mathbb{K}_1 \times \ldots \times \mathbb{K}_r$ such that $x_j \ne -f_1(\alpha_j)$ and $x_j \ne -f_2(\alpha_j)$, $j = 1, \ldots, r$. Again, we remark that $f^*(\alpha_j) = (f(\alpha_j))^{-1}$, $j = 1, \ldots, r$, for any $f \in \mathcal{R}^*$. Thus we obtain

$$\begin{aligned} &\sum_{G\in\mathcal{R}}^* \chi_{\mathbf{a}}((G+f_1)^* - (G+f_2)^*) \\ &\quad = \sum_{G\in\mathcal{R}}^* \prod_{j=1}^r \mathbf{e}\left(\mathrm{Tr}_j \left(a_j \left(G(\alpha_j) + f_1(\alpha_j)\right)^{-1} - a_j \left(G(\alpha_j) + f_2(\alpha_j)\right)^{-1} \right) \right) \\ &\quad = \sum_{(x_1,\ldots,x_r)\in\mathcal{A}_{f_1,f_2}} \prod_{j=1}^r \mathbf{e}\left(\mathrm{Tr}_j \left(a_j \frac{f_2(\alpha_j) - f_1(\alpha_j)}{(x_j + f_1(\alpha_j))(x_j + f_2(\alpha_j))} \right) \right) \\ &\quad = \prod_{j=1}^r \sum_{x_j\in\mathbb{K}_j\setminus\{-f_1(\alpha_j),-f_2(\alpha_j)\}} \mathbf{e}\left(\mathrm{Tr}_j \left(a_j \frac{f_2(\alpha_j) - f_1(\alpha_j)}{(x_j + f_1(\alpha_j))(x_j + f_2(\alpha_j))} \right) \right). \end{aligned}$$

For $j \notin \mathcal{J}$, we bound the inner sum trivially by p^{n_j}. Let $\mathcal{J}_{f_1,f_2} \subseteq \mathcal{J}$ be the set of $j \in \mathcal{J}$ for which $f_1(\alpha_j) \ne f_2(\alpha_j)$. For $j \in \mathcal{J}\setminus\mathcal{J}_{f_1,f_2}$, we can again bound the inner sum by p^{n_j}. Thus we have the estimate

$$\left| \sum_{G\in\mathcal{R}}^* \chi_{\mathbf{a}}((G+f_1)^* - (G+f_2)^*) \right|$$

$$\le \prod_{j \in \mathcal{J}_{f_1,f_2}} \left| \sum_{x_j \in \mathbb{K}_j \setminus \{-f_1(\alpha_j), -f_2(\alpha_j)\}} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j \frac{f_2(\alpha_j) - f_1(\alpha_j)}{(x_j + f_1(\alpha_j))(x_j + f_2(\alpha_j))}\right)\right)\right| \times \prod_{j \notin \mathcal{J}_{f_1,f_2}} p^{n_j}.$$

For sums with $j \in \mathcal{J}_{f_1,f_2}$ we use the Weil bound (in the form given in [4]) which yields

$$\left| \sum_{x_j \in \mathbb{K}_j \setminus \{-f_1(\alpha_j), -f_2(\alpha_j)\}} \mathbf{e}\left(\mathrm{Tr}_j\left(a_j \frac{f_2(\alpha_j) - f_1(\alpha_j)}{(x_j + f_1(\alpha_j))(x_j + f_2(\alpha_j))}\right)\right)\right| \le 3p^{n_j/2},$$

thus

$$\begin{aligned}\left|\sum_{G \in \mathcal{R}}^{*} \chi_{\mathbf{a}}\left((G+f_1)^* - (G+f_2)^*\right)\right| &\le 3^{|\mathcal{J}_{f_1,f_2}|} \prod_{j \in \mathcal{J}_{f_1,f_2}} p^{n_j/2} \prod_{j \notin \mathcal{J}_{f_1,f_2}} p^{n_j} \\ &\le 3^{|\mathcal{J}|} p^{n/2} \prod_{j \notin \mathcal{J}_{f_1,f_2}} p^{n_j/2} \\ &= 3^{|\mathcal{J}|} p^{n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \prod_{j \in \mathcal{J} \setminus \mathcal{J}_{f_1,f_2}} p^{n_j/2}.\end{aligned}$$

Now let $T(m)$ be the number of pairs $(f_1, f_2) \in \mathcal{L}^2$, $f_1 \ne f_2$, such that

$$\sum_{j \in \mathcal{J} \setminus \mathcal{J}_{f_1,f_2}} n_j = m. \tag{8}$$

Collecting together the previous estimates, we obtain

$$W_{\mathbf{a}}(\mathcal{L})^2 \le p^n \left(p^n |\mathcal{L}| + 3^{|\mathcal{J}|} p^{n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \sum_{m=0}^{n} T(m) p^{m/2}\right).$$

It is obvious that for any pair $(f_1, f_2) \in \mathcal{L}^2$, $f_1 \ne f_2$, we have

$$\prod_{j \in \mathcal{J} \setminus \mathcal{J}_{f_1,f_2}} F_j \;\Big|\; f_1 - f_2.$$

Thus for each $f_1 \in \mathcal{L}$ there are at most p^{n-m} polynomials $f_2 \in \mathcal{L}$ satisfying (8). Hence $T(m) \le p^{n-m}|\mathcal{L}|$. Using this inequality for $p^m \ge p^n |\mathcal{L}|^{-1}$ and the trivial estimate $T(m) \le |\mathcal{L}|^2$ otherwise, we see that

$$T(m) p^{m/2} \le p^{n/2} |\mathcal{L}|^{3/2}, \qquad m = 0, \ldots, n.$$

Hence

$$W_{\mathbf{a}}(\mathcal{L})^2 \le p^n \left(p^n |\mathcal{L}| + (n+1) 3^{|\mathcal{J}|} p^n |\mathcal{L}|^{3/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \right).$$

Taking into account that the first term never dominates, we obtain the desired result. □

Clearly, for special sets $\mathcal{L}$ that admit stronger bounds for $T(m)$, one can obtain better results. For example, let us denote by $\mathcal{R}_k$ the set of p^k polynomials $f \in \mathcal{R}$ of degree $\deg f < k$.

Lemma 4 *Let $\mathbf{a} = (a_1, \ldots, a_r) \in \mathcal{A}$ and let $\mathcal{J} \subseteq \{1, \ldots, r\}$ be the set of j with $a_j \ne 0$. Then the bound*

$$W_{\mathbf{a}}(\mathcal{R}_k) \le p^{k+n} \left(p^{-k} + 3^{|\mathcal{J}|+1} p^{-n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \right)^{1/2}$$

holds.

Proof. It is obvious that if $m < k$ then for each $f_1 \in \mathcal{R}_k$ there are at most p^{k-m} polynomials $f_2 \in \mathcal{R}_k$, $f_1 \ne f_2$, that satisfy (8). Hence $T(m) \le p^{2k-m}$, and as in the proof of Lemma 3, we derive

$$\begin{aligned}
W_{\mathbf{a}}(\mathcal{R}_k)^2 &\le p^n \left(p^{k+n} + 3^{|\mathcal{J}|} p^{2k+n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \sum_{m=0}^{k-1} p^{-m/2} \right) \\
&\le p^n \left(p^{k+n} + \frac{1}{1-p^{-1/2}} 3^{|\mathcal{J}|} p^{2k+n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \right) \\
&\le p^n \left(p^{k+n} + \frac{1}{1-3^{-1/2}} 3^{|\mathcal{J}|} p^{2k+n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \right) \\
&\le p^n \left(p^{k+n} + 3^{|\mathcal{J}|+1} p^{2k+n/2} \prod_{j \notin \mathcal{J}} p^{n_j/2} \right).
\end{aligned}$$

The result follows. □

3 Distribution of Inverses

Given a polynomial $g \in \mathcal{R}$ and an integer d, we denote by $N(g,d,h)$ the number of polynomials $f \in \mathcal{R}(h)^*$ such that $\deg(g - f^*) < d$.

Theorem 5 *The bound*

$$\left| N(g,d,h) - \frac{|\mathcal{R}(h)^*|}{p^{n-d}} \right| \le 5^n p^{n/2} (\ln p)^n$$

holds.

Proof. Obviously, $N(g,d,h) = p^{-d} T(g,d,h)$, where $T(g,d,h)$ is number of representations $f^* = g + \psi - \varphi$ with $f \in \mathcal{R}(h)^*$ and polynomials $\varphi, \psi \in \mathcal{R}$ of degree at most $d-1$. From the identity (5) we derive

$$\begin{aligned} T(g,d,h) &= \frac{1}{p^n} \sum_{f \in \mathcal{R}(h)^*} \sum_{\substack{\varphi,\psi \in \mathcal{R} \\ \deg\varphi, \deg\psi \le d-1}} \sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(f^* - g + \varphi - \psi) \\ &= \frac{1}{p^n} \sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(-g) \sum_{f \in \mathcal{R}(h)^*} \chi_{\mathbf{a}}(f^*) \sum_{\substack{\varphi,\psi \in \mathcal{R} \\ \deg\varphi, \deg\psi \le d-1}} \chi_{\mathbf{a}}(\varphi - \psi) \\ &= \frac{1}{p^n} \sum_{\mathbf{a} \in \mathcal{A}} \chi_{\mathbf{a}}(-g) \sum_{f \in \mathcal{R}(h)^*} \chi_{\mathbf{a}}(f^*) \left| \sum_{\substack{\varphi \in \mathcal{R} \\ \deg\varphi \le d-1}} \chi_{\mathbf{a}}(\varphi) \right|^2 . \end{aligned}$$

The term corresponding to $\mathbf{a} = \mathbf{0}$ is equal to $p^{2d-n}|\mathcal{R}(h)^*|$. For any nonempty set $\mathcal{J} \subseteq \{1,\ldots,r\}$, let $\mathcal{A}_{\mathcal{J}}$ be the subset of $\mathcal{A}$ consisting of all $\mathbf{a} = (a_1,\ldots,a_r)$ with $a_j = 0$ for all $j \notin \mathcal{J}$. From Lemma 2 it follows that

$$\begin{aligned} &\left| T(g,d,h) - \frac{|\mathcal{R}(h)^*|}{p^{n-2d}} \right| \\ &\quad \le \frac{1}{p^n} \sum_{\substack{\mathcal{J} \subseteq \{1,\ldots,r\} \\ \mathcal{J} \ne \emptyset}} \sum_{\substack{\mathbf{a} \in \mathcal{A}_{\mathcal{J}} \\ \mathbf{a} \ne \mathbf{0}}} \left| \sum_{f \in \mathcal{R}(h)^*} \chi_{\mathbf{a}}(f^*) \right| \left| \sum_{\substack{\varphi \in \mathcal{R} \\ \deg\varphi \le d-1}} \chi_{\mathbf{a}}(\varphi) \right|^2 \\ &\quad \le \frac{(1+\ln p)^n}{p^{n/2}} \sum_{\substack{\mathcal{J} \subseteq \{1,\ldots,r\} \\ \mathcal{J} \ne \emptyset}} 2^{|\mathcal{J}|} \prod_{j \notin \mathcal{J}} p^{n_j/2} \sum_{\substack{\mathbf{a} \in \mathcal{A}_{\mathcal{J}} \\ \mathbf{a} \ne \mathbf{0}}} \left| \sum_{\substack{\varphi \in \mathcal{R} \\ \deg\varphi \le d-1}} \chi_{\mathbf{a}}(\varphi) \right|^2 . \end{aligned}$$

It is easy to see that

$$\begin{aligned}
&\sum_{\substack{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}\\ \mathbf{a}\neq\mathbf{0}}}\left|\sum_{\substack{\varphi\in\mathcal{R}\\ \deg\varphi\le d-1}}\chi_{\mathbf{a}}(\varphi)\right|^2\\
&\qquad=-p^{2d}+\sum_{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}}\left|\sum_{\substack{\varphi\in\mathcal{R}\\ \deg\varphi\le d-1}}\chi_{\mathbf{a}}(\varphi)\right|^2\\
&\qquad=-p^{2d}+\sum_{\substack{\varphi,\psi\in\mathcal{R}\\ \deg\varphi,\deg\psi\le d-1}}\sum_{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}}\chi_{\mathbf{a}}(\varphi-\psi)\\
&\qquad=-p^{2d}+\sum_{\substack{\varphi,\psi\in\mathcal{R}\\ \deg\varphi,\deg\psi\le d-1}}\sum_{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}}\prod_{j\in\mathcal{J}}\mathbf{e}\left(\mathrm{Tr}_j\left(a_j\left(\varphi\left(\alpha_j\right)-\psi\left(\alpha_j\right)\right)\right)\right)\\
&\qquad=-p^{2d}+U\prod_{j\in\mathcal{J}}p^{n_j},
\end{aligned}$$

where U is the number of pairs $\varphi,\psi\in\mathcal{R}$ with $\deg\varphi,\deg\psi\le d-1$ (that is, $\varphi,\psi\in\mathcal{R}_d$) and such that $\varphi\left(\alpha_j\right)=\psi\left(\alpha_j\right)$ for all $j\in\mathcal{J}$. Since this condition is equivalent to the polynomial congruence

$$\varphi(X)\equiv\psi(X)\pmod{\prod_{j\in\mathcal{J}}F_j(X)},$$

we derive that

$$U=\begin{cases}p^{2d}\prod_{j\in\mathcal{J}}p^{-n_j}, & \text{if } d\ge\sum_{j\in\mathcal{J}}n_j,\\ p^d, & \text{otherwise.}\end{cases}$$

Hence, in either case

$$0\le-p^{2d}+U\prod_{j\in\mathcal{J}}p^{n_j}\le p^d\prod_{j\in\mathcal{J}}p^{n_j},$$

and we derive the inequality

$$\sum_{\substack{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}\\ \mathbf{a}\neq\mathbf{0}}}\left|\sum_{\substack{\varphi\in\mathcal{R}\\ \deg\varphi\le d-1}}\chi_{\mathbf{a}}(\varphi)\right|^2\le p^d\prod_{j\in\mathcal{J}}p^{n_j}. \tag{9}$$

Thus

$$\begin{aligned}
\left|T(g,d,h)-\frac{|\mathcal{R}(h)^*|}{p^{n-2d}}\right| &\le \frac{(1+\ln p)^n p^d}{p^{n/2}} \sum_{\substack{\mathcal{J}\subseteq\{1,\ldots,r\}\\ \mathcal{J}\neq\emptyset}} 2^{|\mathcal{J}|} \prod_{j\notin\mathcal{J}} p^{n_j/2} \prod_{j\in\mathcal{J}} p^{n_j} \\
&= (1+\ln p)^n p^d \sum_{\substack{\mathcal{J}\subseteq\{1,\ldots,r\}\\ \mathcal{J}\neq\emptyset}} 2^{|\mathcal{J}|} \prod_{j\in\mathcal{J}} p^{n_j/2} \\
&= (1+\ln p)^n p^d \left(\prod_{j=1}^{r}\left(1+2p^{n_j/2}\right)-1\right) \\
&\le 2^n(1+\ln p)^n p^{d+n/2} \prod_{j=1}^{r}\left(1+\frac{1}{2p^{n_j/2}}\right) \\
&\le 2^n(1+\ln p)^n p^{d+n/2}\left(1+\frac{1}{2p^{1/2}}\right)^n.
\end{aligned}$$

Therefore

$$\begin{aligned}
\left|N(g,d,h)-\frac{|\mathcal{R}(h)^*|}{p^{n-d}}\right| &= \frac{1}{p^d}\left|T(g,d,h)-\frac{|\mathcal{R}(h)^*|}{p^{n-2d}}\right| \\
&\le 2^n(1+\ln p)^n\left(1+\frac{1}{2p^{1/2}}\right)^n p^{n/2}.
\end{aligned}$$

One easily verifies that

$$2(1+\ln p)\left(1+\frac{1}{2p^{1/2}}\right) < 5\ln p$$

for $p \ge 3$ and the theorem follows (if $p \ge 5$, we can replace 5 by 4 in the preceding inequality). □

In particular, we see from (3) and Theorem 5 that for any $\varepsilon > 0$, there exists a constant $p_0(\varepsilon)$ such that for $p \ge p_0(\varepsilon)$ and $h \ge \max\{n^{1+\varepsilon}, p^{1/2+\varepsilon}\}$, the asymptotic formula $N(g,d,h) \sim (2h+1)^n/p^{n-d}$ holds for any $d \le (1-3\varepsilon)n/2$.

Given polynomials $g, G \in \mathcal{R}$, a set $\mathcal{L} \subseteq \mathcal{R}$ and an integer d we denote by $N(g,d,G,\mathcal{L})$ the number of polynomials $f \in \mathcal{L}_G^*$ such that $\deg(g-f^*) < d$.

Theorem 6 *The bound*

$$\frac{1}{p^n}\sum_{G\in\mathcal{R}}\left|N(g,d,G,\mathcal{L})-\frac{|\mathcal{L}_G^*|}{p^{n-d}}\right| \le 2n^{1/2}3^n|\mathcal{L}|^{3/4}$$

holds.

Proof. As in the proof of Theorem 5, $N(g,d,G,\mathcal{L}) = p^{-d}T(g,d,G,\mathcal{L})$, where $T(g,d,G,\mathcal{L})$ is number of representations $f^* = g + \psi - \varphi$ with $f \in \mathcal{L}_G^*$ and polynomials $\varphi, \psi \in \mathcal{R}$ of degree at most $d-1$. Again we have

$$\left|T(g,d,G,\mathcal{L}) - \frac{|\mathcal{L}_G^*|}{p^{n-2d}}\right| \leq \frac{1}{p^n} \sum_{\substack{\mathcal{J}\subseteq\{1,\ldots,r\}\\ \mathcal{J}\neq\emptyset}} \sum_{\substack{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}\\ \mathbf{a}\neq\mathbf{0}}} \left|\sum_{f\in\mathcal{L}_G^*} \chi_{\mathbf{a}}(f^*)\right| \left|\sum_{\substack{\varphi\in\mathcal{R}\\ \deg\varphi\leq d-1}} \chi_{\mathbf{a}}(\varphi)\right|^2.$$

Thus, from Lemma 3 and the inequality (9), we derive

$$\begin{aligned}
&\sum_{G\in\mathcal{R}} \left|T(g,d,G,\mathcal{L}) - \frac{|\mathcal{L}_G^*|}{p^{n-2d}}\right| \\
&\quad\leq 2n^{1/2}|\mathcal{L}|^{3/4} \sum_{\substack{\mathcal{J}\subseteq\{1,\ldots,r\}\\ \mathcal{J}\neq\emptyset}} 3^{|\mathcal{J}|/2} \prod_{j\notin\mathcal{J}} p^{n_j/4} \sum_{\substack{\mathbf{a}\in\mathcal{A}_{\mathcal{J}}\\ \mathbf{a}\neq\mathbf{0}}} \left|\sum_{\substack{\varphi\in\mathcal{R}\\ \deg\varphi\leq d-1}} \chi_{\mathbf{a}}(\varphi)\right|^2 \\
&\quad\leq 2n^{1/2}|\mathcal{L}|^{3/4} p^{d+n/4} \sum_{\substack{\mathcal{J}\subseteq\{1,\ldots,r\}\\ \mathcal{J}\neq\emptyset}} 3^{|\mathcal{J}|/2} \prod_{j\in\mathcal{J}} p^{3n_j/4} \\
&\quad= 2n^{1/2}|\mathcal{L}|^{3/4} p^{d+n/4} \left(\prod_{j=1}^{r} \left(1 + 3^{1/2}p^{3n_j/4}\right) - 1\right) \\
&\quad\leq 2n^{1/2}3^{n/2}|\mathcal{L}|^{3/4} p^{d+n} \prod_{j=1}^{r} \left(1 + 3^{-1/2}p^{-3n_j/4}\right) \\
&\quad\leq 2n^{1/2}3^{n/2}|\mathcal{L}|^{3/4} p^{d+n} \left(1 + 3^{-1/2}p^{-3/4}\right)^n.
\end{aligned}$$

From the inequality

$$3^{1/2}\left(1 + 3^{-5/4}\right) < 3 \tag{10}$$

the theorem follows. □

Finally, we use Lemma 4 to obtain a similar statement for sets $\mathcal{R}_k$.

Theorem 7 *The bound*

$$\frac{1}{p^n} \sum_{G\in\mathcal{R}} \left|N(g,d,G,\mathcal{R}_k) - \frac{|\mathcal{R}_{k,G}^*|}{p^{n-d}}\right| \leq \left(\frac{4}{3}\right)^n p^{k/2} + 3^{1/2}3^n p^{k-n/4}$$

holds.

Proof. Using the inequality $(x+y)^{1/2} \le x^{1/2} + y^{1/2}$ and applying Lemma 4, we derive as in the proofs of Theorems 5 and 6

$$\begin{aligned}
&\frac{1}{p^n} \sum_{G \in \mathcal{R}} \left| N(g,d,G,\mathcal{R}_k) - \frac{|\mathcal{R}^*_{k,G}|}{p^{n-d}} \right| \\
&\quad \le p^{k-n} \left(p^{-k/2} \sum_{\substack{\mathcal{J} \subseteq \{1,\dots,r\} \\ \mathcal{J} \ne \emptyset}} \prod_{j \in \mathcal{J}} p^{n_j} + 3^{1/2} \sum_{\substack{\mathcal{J} \subseteq \{1,\dots,r\} \\ \mathcal{J} \ne \emptyset}} 3^{|\mathcal{J}|/2} \prod_{j \in \mathcal{J}} p^{3n_j/4} \right) \\
&\quad \le p^{k-n} \left(p^{-k/2} \prod_{j=1}^{r} (1 + p^{n_j}) + 3^{1/2} \prod_{j=1}^{r} \left(1 + 3^{1/2} p^{3n_j/4}\right) \right) \\
&\quad \le p^{k-n} \left(p^{n-k/2} \prod_{j=1}^{r} \left(1 + p^{-n_j}\right) + 3^{(n+1)/2} p^{3n/4} \prod_{j=1}^{r} \left(1 + 3^{-1/2} p^{-3n_j/4}\right) \right) \\
&\quad \le p^{k-n} \left(\left(1 + p^{-1}\right)^n p^{n-k/2} + 3^{(n+1)/2} (1 + 3^{-1/2} p^{-3/4})^n p^{3n/4} \right) \\
&\quad \le \left(1 + p^{-1}\right)^n p^{k/2} + 3^{(n+1)/2} (1 + 3^{-1/2} p^{-3/4})^n p^{k-n/4}.
\end{aligned}$$

From the inequality (10) the theorem follows. □

4 Remarks

It is easy to see that for larger values of p the constants in the above estimates can be slightly improved. For example, if $p \ge 5$ the bound of Theorem 5 holds with 5^n replaced by 4^n. If $p \ge 7$, the bounds of Theorems 6 and 7 hold with 3^n replaced by 2^n and with $(4/3)^n$ replaced by $(8/7)^n$ (in Theorem 7). Moreover for any $\varepsilon > 0$ there exists $p_0(\varepsilon)$ such that for $p > p_0(\varepsilon)$ one can take $(2+\varepsilon)^n$ instead of 5^n in Theorem 5, $(3^{1/2}+\varepsilon)^n$ instead of 3^n in Theorems 6 and 7, and $(1+\varepsilon)^n$ instead of $(4/3)^n$ in Theorem 7.

As we have mentioned, it would be very important to obtain results about the distribution of inverses f^*, $f \in \mathcal{R}(h)^*$, for smaller values of h. The case $F(X) = X^n - 1$ is of primary interest.

It would also be interesting to estimate the number of $f \in \mathcal{R}(h)^*$ such that $f^* \in \mathcal{R}(H)$ for the smallest possible values of h and H. The techniques of the present paper can be used to derive such results in the case where $F(X)$ is an irreducible polynomial (and $h \cdot H \ge p^{3/2+\varepsilon}$), but it is not clear how

to approach a more general class of polynomials, including the polynomial $F(X) = X^n - 1$.

Finally, it would be of interest to study residue rings modulo arbitrary polynomials $F(X)$ that are not necessarily square-free.

References

[1] E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.

[2] J. Hoffstein, J. Pipher and J. H. Silverman, 'NTRU: A ring based public key cryptosystem', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1433** (1998), 267–288.

[3] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[4] C. J. Moreno and O. Moreno, 'Exponential sums and Goppa codes, 1', *Proc. Amer. Math. Soc.*, **111** (1991), 523–531.

[5] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[6] J. H. Silverman, 'Invertibility in truncated polynomial rings', *NTRU Cryptosystem Tech. Report 9*, 1998, 1–8.

[7] I. M. Vinogradov, *Elements of number theory*, Dover Publ., New York, 1954.