Hindawi Publishing Corporation
Journal of Discrete Mathematics
Volume 2014, Article ID 263179, 4 pages
http://dx.doi.org/10.1155/2014/263179

Research Article

Counting Irreducible Polynomials of Degree r over $\mathbb{F}_{q^n}$ and Generating Goppa Codes Using the Lattice of Subfields of $\mathbb{F}_{q^{nr}}$

Kondwani Magamba[1] and John A. Ryan[2]

[1] *Malawi Institute of Technology, Malawi University of Science and Technology, P.O. Box 5196, Limbe, Malawi*
[2] *Department of Mathematics, Mzuzu University, Private Bag 201, Luwinga, Mzuzu, Malawi*

Correspondence should be addressed to Kondwani Magamba; kondwanimagamba@gmail.com

Received 28 May 2014; Accepted 8 September 2014; Published 18 September 2014

Academic Editor: Jean-Pierre Gazeau

The problem of finding the number of irreducible monic polynomials of degree r over $\mathbb{F}_{q^n}$ is considered in this paper. By considering the fact that an irreducible polynomial of degree r over $\mathbb{F}_{q^n}$ has a root in a subfield $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^{nr}}$ if and only if $(nr/s, r) = 1$, we show that Gauss's formula for the number of monic irreducible polynomials can be derived by merely considering the lattice of subfields of $\mathbb{F}_{q^{nr}}$. We also use the lattice of subfields of $\mathbb{F}_{q^{nr}}$ to determine if it is possible to generate a Goppa code using an element lying in a proper subfield of $\mathbb{F}_{q^{nr}}$.

1. Introduction

In this paper we consider the problem of finding the number, $|\mathscr{P}_r|$, of monic irreducible polynomials of degree r over the field $\mathbb{F}_{q^n}$, where n is a positive integer and q is the power of a prime number. This problem has been discussed by several authors including C. F. Gauss who gave the following beautiful formula:

$$|\mathscr{P}_r| = \frac{1}{r}\sum_{d|r}\mu(d)\, q^{nr/d}, \tag{1}$$

where d runs over the set of all positive divisors of r including 1 and r and $\mu(k)$ is the Möbius function; see [1]. Recently, it has been shown, see [2], that this number can be found by using only basic facts about finite fields and the Principle of Inclusion-Exclusion. This work seeks to emphasize the simplicity of the method given in [2] by using a lattice of subfields. This is done by first of all proving Gauss's formula using the Principle of Inclusion-Exclusion as was done in [2]. However, we use only one basic fact about where (in which subfields) the roots of irreducible polynomials of degree r over $\mathbb{F}_{q^n}$ can lie. We then show how a lattice of subfields of the field, $\mathbb{F}_{q^{nr}}$, can be used to obtain $|\mathscr{P}_r|$. We are particularly interested in the number of roots of irreducible polynomials of degree r over $\mathbb{F}_{q^n}$ because the problem of counting irreducible Goppa codes of length q^n and of degree r depends on this number.

2. Preliminaries

2.1. The Number of Irreducible Polynomials. Our approach to counting the number of irreducible polynomials of degree r over $\mathbb{F}_{q^n}$ is to count the number of all roots of such polynomials. To this end, we make the following definitions.

Definition 1. One defines the set $\mathbb{S}(n, r)$ to be the set of all elements in $\mathbb{F}_{q^{nr}}$ of degree r over $\mathbb{F}_{q^n}$.

Definition 2. One defines the set $\mathscr{P}_r$ to be the set of all irreducible monic polynomials of degree r over $\mathbb{F}_{q^n}$.

The following theorem is well known.

Theorem 3. $|\mathscr{P}_r|$ *is given by formula* (1).

For the sake of clarity we state the relationship between $\mathscr{P}_r$ and $\mathbb{S}(n, r)$ which immediately leads to the "Gaussian like"

count of the number of elements in $\mathbb{S}(n,r)$. We put this in the following corollary.

Corollary 4. *$\mathbb{S}(n,r)$ is the union of all the roots of the polynomials in $\mathcal{P}_r$ and*

$$|\mathbb{S}(n,r)| = \sum_{d|r} \mu(d)\, q^{nr/d}. \tag{2}$$

2.2. Where Elements of $\mathbb{S}(n,r)$ Lie. We next identify the subfields of $\mathbb{F}_{q^{nr}}$ where the elements of $\mathbb{S}(n,r)$ lie. To achieve this we first note that an irreducible polynomial over $\mathbb{F}_{q^n}$ may, in some specific cases, be seen as irreducible over an extension field of $\mathbb{F}_{q^n}$. To be more specific, we state this in the following theorem.

Theorem 5. *An irreducible polynomial over $\mathbb{F}_{q^n}$ of degree r remains irreducible over $\mathbb{F}_{q^{nt}}$ if and only if $(r,t) = 1$; see [3].*

Now, in order to apply Theorem 5 to general cases, one makes the following decompositions of n and r.

Definition 6. One defines k to be the largest divisor of n that is relatively prime to r and set $l_n = n/k$ and defines m to be the largest divisor of r that is relatively prime to n and set $l_r = r/m$. Thus $nr = kl_nl_rm = klm$, where $l = l_nl_r$.

With this notation, the following lemma is a direct result of Theorem 5.

Lemma 7. *$\mathbb{S}(n,r)$ consists of the elements of $\mathbb{F}_{q^{nr}}$ each of which is a root of an irreducible polynomial of degree r over $\mathbb{F}_{q^{k_1l_n}}$, where k_1 is a divisor of k. In particular, the elements of $\mathbb{S}(n,r)$ are precisely those elements that lie in a subfield of $\mathbb{F}_{q^{nr}}$ of the form $\mathbb{F}_{q^{k_1l_nr}}$, for some k_1, but not in any subfield of the form $\mathbb{F}_{q^s}$, where s is not divisible by l_nr. See [4].*

It is useful, for our purposes, to think of the subfields identified in Lemma 7 in the following way.

Corollary 8. *The subfields of the form $\mathbb{F}_{q^s}$ defined in Lemma 7 are the maximal subfields of $\mathbb{F}_{q^{nr}}$ such that $(nr/s, r) \neq 1$ or the subfields contained in such maximal subfields.*

2.3. The Principle of Inclusion-Exclusion. Since we will be making extensive use of the "Principle of Inclusion-Exclusion" we state this well known principle in the following theorem; see [5].

Theorem 9. *Let $A_1, A_2, \ldots, A_n$ be finite sets. Then*

$$\begin{aligned}\left|A_1 \cup A_2 \cup \cdots \cup A_n\right| = {} & \sum_{1\le i\le n} \left|A_i\right| - \sum_{1\le i<j\le n} \left|A_i \cap A_j\right| \\ & + \sum_{1\le i<j<k\le n} \left|A_i \cap A_j \cap A_k\right| \\ & - \cdots + (-1)^{n+1} \left|A_1 \cap A_2 \cap \cdots \cap A_n\right|.\end{aligned} \tag{3}$$

2.4. Goppa Codes. This paper is motivated by the unsolved problem of finding an irreducible polynomial which defines a "good" Goppa code of degree r and length q^n or equivalently finding an element of degree r which defines such a code. So it is appropriate for us to define a Goppa code. The following definition is the classical definition found in much of the literature on coding theory.

Definition 10. Let $g(z) \in \mathbb{F}_{q^n}[z]$ be irreducible of degree r and let $L = \mathbb{F}_{q^n} = \{\zeta_i : 0 \le i \le q^n - 1\}$. Then the irreducible Goppa code $\Gamma(L,g)$ is defined as the set of all vectors $\underline{c} = (c_0, c_1, \ldots, c_{q^n-1})$ with components in $\mathbb{F}_q$ which satisfy the condition

$$\sum_{i=0}^{q^n-1} \frac{c_i}{z-\zeta_i} \equiv 0 \bmod g(z). \tag{4}$$

The polynomial $g(z)$ is called the Goppa polynomial. Since $g(z)$ is irreducible and of degree r over $\mathbb{F}_{q^n}$, $g(z)$ does not have any root in L and the code is called an irreducible Goppa code of degree r. In this paper $g(z)$ is always irreducible of degree r over $\mathbb{F}_{q^n}$.

2.4.1. Irreducible Goppa Codes Defined by a Field Element. The following characterization of an irreducible Goppa code is particularly useful for our purposes. It can be shown, see [6], that if α is any root of the Goppa polynomial $g(z)$ then $\Gamma(L,g)$ is completely described by any root α of $g(z)$ and a parity check matrix $\mathbf{H}(\alpha)$ is given by

$$\mathbf{H}(\alpha) = \left(\frac{1}{\alpha-\zeta_0}\frac{1}{\alpha-\zeta_1}\cdots\frac{1}{\alpha-\zeta_{q^n-1}}\right). \tag{5}$$

We denote this code by $C(\alpha)$. Since $C(\alpha)$ is completely described by the root α of $g(z)$ the number $|\mathbb{S}|$ gives an upper bound on the number of irreducible Goppa codes. Furthermore, knowing the various locations (subfields) of the elements of $\mathbb{S}$ will facilitate research into finding the element which will give the best Goppa code.

3. Proof of Gauss's Formula

We now give a new proof of Gauss's Formula when applied to find the cardinality of the set $\mathbb{S}$ which has special significance in the application to Goppa codes. Putting $n = 1$ in our proof will give the result proved in [2]. There are many similarities between approach given in [2] and our method. However, the crux of our argument lies on Corollary 8 which in turn is based on Theorem 5. We believe that this slightly different approach brings a little more clarity to the situation.

Proof. Let $r = r_1^{i_1} r_2^{i_2} \cdots r_w^{i_w}$ be the prime factorisation of r. The maximal subfields $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^{nr}}$, as in Corollary 8, are of the form

$$\mathbb{F}_{q^{nr/r_1}}, \mathbb{F}_{q^{nr/r_2}}, \ldots, \mathbb{F}_{q^{nr/r_w}}. \tag{6}$$

Thus, by Corollary 8, $|\mathbb{S}(n,r)| = |(\mathbb{F}_{q^{nr/r_1}} \cup \mathbb{F}_{q^{nr/r_2}} \cup \cdots \cup \mathbb{F}_{q^{nr/r_w}})'|$, where the complement is taken in $\mathbb{F}_{q^{nr}}$. As in [2], we note that $\mathbb{F}_{q^{nr/r_1}} \cap \mathbb{F}_{q^{nr/r_2}} = \mathbb{F}_{q^{nr/r_1r_2}}$,

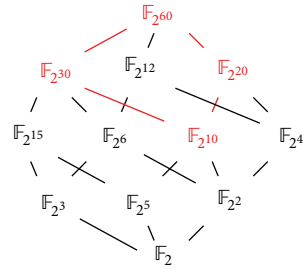

Figure 1: Lattice of subfields of $\mathbb{F}_{2^{60}}$.

$\mathbb{F}_{q^{nr/r_1}} \cap \mathbb{F}_{q^{nr/r_2}} \cap \mathbb{F}_{q^{nr/r_3}} = \mathbb{F}_{q^{nr/r_1r_2r_3}}$, and so forth. Using the Principle of Inclusion-Exclusion, it follows that

$$\begin{aligned} |\mathbb{S}(n,r)| &= q^{nr} - q^{nr/r_1} - q^{nr/r_2} - \cdots - q^{nr/r_w} \\ &\quad + q^{nr/r_1r_2} + q^{nr/r_1r_3} + \cdots + q^{nr/r_{w-1}r_w} \\ &\quad \vdots \\ &\quad + (-1)^w q^{nr/r_1r_2\cdots r_w}. \end{aligned} \tag{7}$$

Finally, note that $|\mathscr{P}_r| = |\mathbb{S}(n,r)|/r$. □

4. $|\mathscr{P}_r|$ Using a Lattice of Subfields of $\mathbb{F}_{q^{nr}}$

We have noted that in order to construct $\mathbb{S}(n,r)$ a lattice of subfields of $\mathbb{F}_{q^{nr}}$ together with Corollary 8 offers a good insight into $\mathbb{S}(n,r)$. We will put the lattice of subfields of $\mathbb{F}_{q^{nr}}$ into their usual hierarchies, where level one is taken by $\mathbb{F}_{q^{nr}}$, and level two contains subfields of $\mathbb{F}_{q^{nr}}$ of the form $\mathbb{F}_{q^{nr/u_i}}$, where $nr = u_1^{i_1}u_2^{i_2}\cdots u_j^{i_j}$ is the prime factorization of nr. Level three comprises of maximal subfields of the fields in level two and so on. As this is done, all intersections between subfields are marked as this is used in getting $\mathbb{S}(n,r)$.

Observe that the elements of $\mathbb{F}_{q^s}$ (those not lying in $\mathbb{S}$) described in Corollary 8 are those which lie in subfields of type $\mathbb{F}_{q^{nr/r_i}}$, where r_i is a prime divisor of r. We can see the formula for $\mathbb{S}(n,r)$ taking shape as we have the full splitting field $\mathbb{F}_{q^{nr}}$ of all the irreducible polynomials of degree r over $\mathbb{F}_{q^n}$, the maximal subfields $\mathbb{F}_{q^{nr/r_i}}$, and the subfields of $\mathbb{F}_{q^{nr/r_i}}$.

Formula (7) shows the levels mentioned above. The subfields that need to be considered in order to find $|\mathbb{S}(n,r)|$ can be read off from a lattice of subfields of $\mathbb{F}_{q^{nr}}$ in accordance with Corollary 8, that is, subfields of the form $\mathbb{F}_{q^{k_1l_nr}}$. We illustrate this method with an example.

Example 11. Let us take $q = 2$, $n = 10$, and $r = 6$. Then, $k = 5$, $l_n = l_r = 2$, $m = 3$, and $\mathbb{F}_{q^{nr}} = \mathbb{F}_{2^{60}}$. Hence the subfields in level two which do not contain any elements of $\mathbb{S}$ (subfields of the form $\mathbb{F}_{q^{nr/r_i}}$) are $\mathbb{F}_{2^{30}}$ and $\mathbb{F}_{2^{20}}$. While the only proper subfield which does contain elements of $\mathbb{S}$ (subfield of the form $\mathbb{F}_{q^{k_1l_nr}}$) is $\mathbb{F}_{2^{12}}$, putting $k_1 = 1$. So in constructing the set $\mathbb{S}$ it is necessary to exclude the two subfields $\mathbb{F}_{2^{30}}$ and $\mathbb{F}_{2^{20}}$. In level three, we will consider the intersection $\mathbb{F}_{2^{30}} \cap \mathbb{F}_{2^{20}} = \mathbb{F}_{2^{10}}$ as this has been excluded twice. Thus, the number of elements of degree 6 over $\mathbb{F}_{2^{10}}$ is $2^{60} - 2^{30} - 2^{20} + 2^{10}$. The lattice shown in Figure 1 illustrates this example.

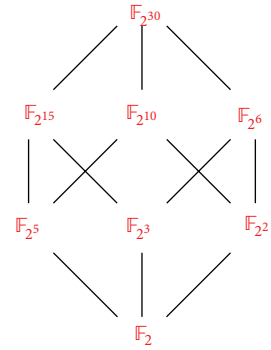

Figure 2: Lattice of subfields of $\mathbb{F}_{2^{30}}$.

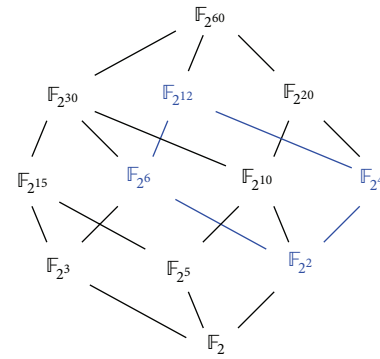

Figure 3: Lattice of subfields of $\mathbb{F}_{2^{60}}$.

Example 12. Let us take $q = 2$, $r = 30$, and $n = 1$. In this case $k = l_n = 1$ and $r = 30$. There are no proper subgroups of the form $\mathbb{F}_{q^{k_1l_nr}}$ but rather all maximal subgroups are of the form $\mathbb{F}_{q^{nr/r_i}}$ and so by Corollary 8 all these maximal subgroups are excluded when constructing the set $\mathbb{S}$. By the Principle of Inclusion-Exclusion, it follows that $|\mathbb{S}(1,30)| = 2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 - 2$. See Figure 2.

5. Applications to Goppa Codes

We know that an irreducible Goppa code, $C(\alpha)$, is defined by a root α of the Goppa polynomial which is of degree r over $\mathbb{F}_{q^n}$. Now to find such an α one can search in any of the subfields of the form $\mathbb{F}_{q^{k_1l_nr}}$. This makes the search easier. We can use a lattice of subfields of $\mathbb{F}_{q^{nr}}$ not only to facilitate this search but also to calculate the number of such elements.

Example 13. Let us look again at the example above with $q = 2$, $n = 10$, and $r = 6$. $\mathbb{F}_{2^{12}}$ contains elements of $\mathbb{S}(10,6)$. The number of elements in $\mathbb{S}(10,6) \cap \mathbb{F}_{2^{12}}$ can be easily calculated from the lattice of subfields. It is $2^{12} - 2^6 - 2^4 + 2^2$. See Figure 3.

6. Conclusion

In this paper we have shown how a lattice of subfields can be used as an alternative to Gauss's formula for finding the number of monic irreducible polynomials of degree r

over $\mathbb{F}_{q^n}$. The lattice of subfields approach helps to clear the mystery surrounding the rather complicated looking Gaussian formula which involves the Möbius function. We have also shown how this method can be used to obtain a Goppa code $C(\alpha)$, where α lies in a lower field. Using the Principle of Inclusion-Exclusion with the lattice of subfields it is easy to calculate the number of such elements α in any subfield. The lattice of subfields approach simplifies the task of finding Goppa codes and sheds light on the processes involved.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] C. F. Gauss, *Untersuchungen Über Höhere Arithmetik*, Chelsea Publishing, New York, NY, USA, 2nd edition, 1981.

[2] S. K. Chebolu and J. Mináč, "Counting irreducible polynomials over finite fields using the inclusion-exclusion principle," *Mathematics Magazine*, vol. 84, no. 5, pp. 369–371, 2011.

[3] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, UK, 1994.

[4] J. A. Ryan and P. Fizpatrick, "Enumeration of inequivalent irreducible Goppa codes," *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 399–412, 2006.

[5] K. H. Rosen, *Discrete Mathematics and Its Applications*, McGraw-Hill, New York, NY, USA, 1999.

[6] C. L. Chen, "Equivalent irreducible Goppa codes," *IEEE Transactions on Information Theory*, vol. 24, no. 6, pp. 766–769, 1978.