J. Austral. Math. Soc. **71** (2001), 299–305

COUNTING IRREDUCIBLE GOPPA CODES

PATRICK FITZPATRICK and JOHN A. RYAN

To Laci Kovács on his 65th birthday

(Received 9 July 2001)

Communicated by R. A. Bryce

Abstract

We consider irreducible Goppa codes of length q^m over $\mathbb{F}_q$ defined by polynomials of degree r, where $q = p^t$ and p, m, r are distinct primes. The number of such codes, inequivalent under coordinate permutations and field automorphisms, is determined.

2000 *Mathematics subject classification*: primary 94B60, 11T71.
Keywords and phrases: classical Goppa codes, enumeration.

1. Introduction

Apart from their intrinsic interest, irreducible Goppa codes are of particular importance because of their application in public-key cryptosystems, since the McEliece cryptosystem [8, page 1217] is based on such a code. However, not all irreducible polynomials of a given degree over a finite field generate inequivalent codes and so it is of interest to investigate how many distinct codes can be generated in this way (see Gibson [4]). Chin-Long Chen [2] gives an upper bound for the number of such codes which is not tight. In this paper we give an improved bound for Goppa codes of length q^m, defined by irreducible polynomials of degree r, where $q = p^t$ and p, m, r are distinct primes. We call such codes G-codes for short. To avoid trivial cases we insist that $r + 1 \leq q^m - 1$, and if $q = 2$ that $2r + 1 \leq 2^m - 1$.

This paper was presented at the Workshop on Coding and Cryptography, WCC2001, Paris, January, 2001.

© 2001 Australian Mathematical Society 0263-6115/2001 $A2.00 + 0.00

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

Our aim is to count G-codes up to equivalence under coordinate permutations and field automorphisms of $\mathbb{F}_q$ (where the same automorphism is applied to each component of a codeword: $\rho(c_1, \ldots, c_{q^m}) = (\rho(c_1), \ldots, \rho(c_{q^m}))$ for $\rho \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$). It is easy to prove that Goppa codes are transformed into Goppa codes by these operations. It does not seem likely that a monomial transformation (over $\mathbb{F}_q$), which is not a scalar multiple of a permutation, sends one Goppa code to another one, but we have not been able to establish this definitively. If it is indeed the case then the result that we establish will give the number of Goppa codes up to the usual definition of equivalence of codes. In particular, this holds for binary codes (see [3]).

2. Preliminaries

Let $g(x)$ be a polynomial defining a G-code and let η be a fixed primitive element of $\mathbb{F}_{q^m}$. It is well known (see [2]) that a G-code is equivalent by a coordinate permutation to one with a parity check matrix of the form

$$\begin{pmatrix} \frac{1}{\alpha} & \frac{1}{\alpha-\eta^0} & \frac{1}{\alpha-\eta} & \cdots & \frac{1}{\alpha-\eta^{q^m-2}} \end{pmatrix} \tag{1}$$

where α is any root of $g(x)$ in its splitting field $\mathbb{F}_{q^{mr}}$. We will say that this code is *defined* by α and denote it by $C(\alpha)$. We denote $\mathbb{F}_{q^{mr}} - \mathbb{F}_{q^m}$ by $\mathbb{S}$. Since r is prime each $\alpha \in \mathbb{S}$ defines a G-code.

We begin with the basic connections between G-codes defined by the elements of $\mathbb{S}$. The following result is well-known ([1, 3, 7]). The converse of this theorem for binary codes is proved in [3].

THEOREM 2.1. *If $\alpha, \beta \in \mathbb{S}$ are related by an equation of the form*

$$\beta = \zeta\alpha^{q^i} + \xi, \quad \text{for } \zeta, \xi \in \mathbb{F}_{q^m},\ \zeta \neq 0,$$

then $C(\alpha)$ and $C(\beta)$ are equivalent G-codes.

The letters ζ, ξ will be reserved throughout for elements of $\mathbb{F}_{q^m}$ with $\zeta \neq 0$. We wish therefore to count the number of orbits of $\mathbb{S}$ under the action of the group generated by the affine transformations $\alpha \to \zeta\alpha + \xi$ and the Frobenius automorphism $\sigma : \alpha \to \alpha^q$.

Consider first the action of the affine group. If $\zeta_1\alpha + \xi_1 = \zeta_2\alpha + \xi_2$ and $\zeta_1 = \zeta_2$, then $\xi_1 = \xi_2$, while if $\zeta_1 \neq \zeta_2$, then $\alpha = (\xi_1 - \xi_2)/(\zeta_1 - \zeta_2)$, contrary to $\alpha \in \mathbb{S}$. Thus each orbit A of the affine group, or *affine set*, contains $q^m(q^m - 1)$ elements. We denote the set of affine sets contained in $\mathbb{S}$ by $\mathbb{A}$ and the affine set containing α by $A(\alpha)$. It follows that $|\mathbb{A}| = (q^{mr} - q^m)/q^m(q^m - 1) = (q^{m(r-1)} - 1)/(q^m - 1)$. Also

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

if $r = 2$, then there is just one affine set containing all $q^{2m} - q^m$ elements of $\mathbb{S}$. Since there is nothing left to do in this case we exclude it and from now on assume that r is odd.

Next, we observe that σ permutes the affine sets since if $\beta = \zeta\alpha + \xi$ then $\beta^q = \zeta^q\alpha^q + \xi^q$. Thus, it remains to consider the orbits of $\mathbb{A}$ under the action of the cyclic group of order mr generated by σ. This group is the direct product of subgroups $R = \langle\sigma^m\rangle$ of order r and $M = \langle\sigma^r\rangle$ of order m. Thus we can consider the actions of these subgroups separately and note that in each case there are only two possibilities for the lengths of the orbits.

3. Action of R

The orbits of $\mathbb{A}$ under R have length 1 or r. Suppose first that A is left invariant by R. The action of R on A also has orbits of length 1 or r, so suppose that $\alpha \in A$ satisfies $\alpha^{q^m} = \alpha$. Then $\alpha^{q^m-1} = 1$ and $\alpha \in \mathbb{F}_{q^m}$ contrary to hypothesis. Thus, the orbits all have length r and A contains all the q^m-conjugates of all of its elements. This also implies $r \mid q^m(q^m - 1)$ and, since r and $q = p^t$ are relatively prime, $r \mid q^m - 1$.

Conversely, suppose $r \mid q^m - 1$. Consider the relation

$$\begin{aligned} q^{mr} - 1 &= (q^m - 1)(q^{m(r-1)} + \cdots + q^m + 1) \\ &= (q^m - 1)[(q^{m(r-1)} - 1) + \cdots + (q^m - 1) + 1 + (r - 1)] \\ &= (q^m - 1)[(q^{m(r-1)} - 1) + \cdots + (q^m - 1) + r]. \end{aligned}$$

Each summand in the second factor on the right is divisible by r and hence $r(q^m - 1) \mid q^{mr} - 1$. It follows that there is an element α of order $r(q^m - 1)$ in $\mathbb{S}$ and $\alpha^{q^m-1} = \varepsilon$, being of order r, lies in $\mathbb{F}_{q^m}$. Now $\varepsilon\alpha = \alpha^{q^m}, \varepsilon^2\alpha = \varepsilon\alpha^{q^m} = (\varepsilon\alpha)^{q^m} = \alpha^{q^{2m}}, \ldots, \varepsilon^{r-1}\alpha = \alpha^{q^{m(r-1)}}$. Also, for any element $\beta = \zeta\alpha + \xi \in A(\alpha)$, we have $\beta^{q^{mi}} = (\zeta\alpha + \xi)^{q^{mi}} = \zeta\alpha^{q^{mi}} + \xi \in A(\alpha)$. Thus $A(\alpha)$ contains all the q^m-conjugates of all its elements and we deduce that $A(\alpha)$ is fixed by R. We summarize in the following theorem.

THEOREM 3.1. *Let A be an affine set. The following are equivalent:*

(i) *there exists an affine set A that is fixed by R;*

(ii) *there exists an affine set A containing an element α such that $\alpha^{q^m-1} = \varepsilon$ has order r in $\mathbb{F}_{q^m}$;*

(iii) $r \mid q^m - 1$.

Now suppose that $r \mid q^m - 1$ and $A = A(\alpha)$ satisfies the hypotheses of the theorem with $\alpha^{q^m-1} = \varepsilon \in \mathbb{F}_{q^m}$ of order r. We wish to count how many such affine sets there are.

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

Each equation $x^{q^m-1} = \varepsilon^j$, $j = 0, \ldots, r-1$ has $q^m - 1$ distinct solutions in $\mathbb{F}_{q^{mr}}$. Of these, $q^m - 1$, corresponding to $j = 0$, lie in $\mathbb{F}_{q^m}$. The remaining $(r-1)(q^m-1)$ lie in $\mathbb{S}$. Observing that $(\zeta\alpha)^{q^m-1} = \alpha^{q^m-1} = \varepsilon$ for all $\zeta \in \mathbb{F}_{q^m}^*$, we see that A contains the $q^m - 1$ solutions of $x^{q^m-1} = \varepsilon$, and it is easy to check that A comprises the q^m translates of this set by $\xi \in \mathbb{F}_{q^m}$. Now $(\alpha^j)^{q^m-1} = \varepsilon^j$ and it is immediate that the affine set $A(\alpha^j)$, $1 \le j \le r-1$, contains the $q^m - 1$ solutions of $x^{q^m-1} = \varepsilon^j$. Hence these sets account for all of the solutions of these equations and we deduce that there are precisely $r-1$ affine sets fixed by R.

The remaining $(q^{m(r-1)} - 1)/(q^m - 1) - r + 1$ affine sets divide into orbits of length r, each of which has the form $\{A(\alpha), A(\alpha^{q^m}) \ldots, A(\alpha^{q^{m(r-1)}})\}$. By a direct verification there are $\sum_{i=1}^{r-2}(q^{mi} - 1)/r$ such orbits.

THEOREM 3.2. *If $r \mid q^m - 1$, then, under the action of R, $\mathbb{A}$ consists of $r-1$ orbits of length 1 and $\sum_{i=1}^{r-2}(q^{mi} - 1)/r$ orbits of length r. If $r \nmid q^m - 1$ then $\mathbb{A}$ consists of $(q^{m(r-1)} - 1)/(r(q^m - 1))$ orbits of length r.*

4. Action of M

We shall often use, without comment, the elementary fact that if u, v are positive integers with gcd d, then $\gcd(x^u - 1, x^v - 1) = x^d - 1$ (see [6, Corollary 3.7], for example).

The orbits of M have length 1 or m. Consider the elements $\alpha \in \mathbb{S}$ fixed by M and therefore satisfying $\alpha^{q^r} = \alpha$, or $\alpha^{q^r-1} = 1$. Suppose α and $\beta = \zeta\alpha + \xi$ are fixed by M. Then $\beta = \beta^{q^r} = \zeta^{q^r}\alpha^{q^r} + \xi^{q^r} = \zeta^{q^r}\alpha + \xi^{q^r}$. If $\zeta^{q^r} \ne \zeta$ this gives $\alpha = (\xi^{q^r} - \xi)/(\zeta - \zeta^{q^r})$ contrary to $\alpha \notin \mathbb{F}_{q^m}$. Thus, $\zeta^{q^r} = \zeta$, which implies that ζ lies in $\mathbb{F}_{q^r} \cap \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^{mr}}$, and hence in $\mathbb{F}_q$. Similarly, $\xi \in \mathbb{F}_q$. Conversely, if $\zeta, \xi \in \mathbb{F}_q$, with $\zeta \ne 0$, and α is fixed by M, then $(\zeta\alpha + \xi)^{q^r} = \zeta\alpha + \xi$, so $\zeta\alpha + \xi$ is fixed by M. It follows that there are $q(q-1)$ fixed points of M in $A = A(\alpha)$. Next, for any $\zeta, \xi \in \mathbb{F}_{q^m}$, $\zeta \ne 0$, we have $(\zeta\alpha + \xi)^{q^r} = \zeta^{q^r}\alpha + \xi^{q^r}$ so $A(\alpha)$ is fixed by M, and the $q^m(q^m - 1) - q(q-1)$ elements, apart from the fixed points, are permuted in orbits of length m. There are $q^r - q$ elements $\alpha \in \mathbb{S}$ satisfying $\alpha^{q^r-1} = 1$ and hence there are

$$\frac{q^r - q}{q(q-1)} = \frac{q^{r-1} - 1}{q - 1}$$

affine sets fixed by M.

If $m \nmid q^m(q^m - 1)$, that is, if $m \nmid q^m - 1$, then each set fixed by M must contain at least one fixed point and therefore $q(q-1)$ fixed points. However, even if $m \mid q^m - 1$, which implies $m \mid \gcd(q^m - 1, q^{m-1} - 1) = q - 1$, we claim that any affine set fixed by M must contain a fixed point. Thus, the only sets fixed by M are those just described.

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

Suppose, therefore, that $m \mid q^m - 1$ and that $\mathbb{A}(\alpha)$ is fixed by M. Let $\alpha^{q^r} = \zeta\alpha + \xi$. We claim that we may assume $\zeta = 1$, that is, that there are $\mu, \nu \in \mathbb{F}_{q^m}$ such that $(\mu\alpha + \nu)^{q^r} = (\mu\alpha + \nu) + \xi'$, for some $\xi' \in \mathbb{F}_{q^m}$. We have $(\mu\alpha + \nu)^{q^r} = \mu^{q^r}\alpha^{q^r} + \nu^{q^r} = \mu^{q^r}(\zeta\alpha + \xi) + \nu^{q^r} = \mu^{q^r-1}\zeta(\mu\alpha + \nu) - \mu^{q^r-1}\zeta\nu + \mu^{q^r}\xi + \nu^{q^r}$. Now if $\zeta \in \mathbb{F}_q^*$, then $\alpha^{q^{2r}} = (\zeta\alpha + \xi)^{q^r} = \zeta^{q^r}\alpha^{q^r} + \xi^{q^r} = \zeta(\zeta\alpha + \xi) + \xi^{q^r} = \zeta^2\alpha + \zeta\xi + \xi^{q^r}$ and, continuing in this way, we arrive at $\alpha = \alpha^{q^{rm}} = \zeta^m\alpha + f(\zeta, \xi)$, where $f(\zeta, \xi)$ is an expression in ζ and ξ only. This means $\zeta^m = 1$ (otherwise $\alpha \in \mathbb{F}_{q^m}$ as before). Since $m \mid q - 1$, we can use the same argument as in Section 3 to see that $m(q-1) \mid q^m - 1$, so there is a $\beta \in \mathbb{F}_{q^m}$ such that $\beta^{q-1} = \zeta^{-1}$. Now, $\gcd(q^m - 1, q^r - 1) = q - 1$ so $m \nmid q^{r-1} + \cdots + q + 1$. Thus there is a j such that $j(q^{r-1} + \cdots + q + 1) \equiv 1 \bmod m$. Defining $\mu = \beta^j$ gives us $\mu^{q^r-1} = \zeta^{-1}$. On the other hand, if the order k of ζ does not divide $q - 1$, then it divides $q^{m-1} + q^{m-2} + \cdots + q + 1$, so $(k, q^r - 1) = 1$, and we can find a j such that $-j(q^r - 1) \equiv -1 \bmod k$. With this j, $(\zeta^{-j})^{q^r-1} = \zeta^{-1}$, so we can choose $\mu = \zeta^{-j}$.

Hence, we may assume that $\alpha^{q^r} = \alpha + \xi$. If $\xi = 0$, then we are done so suppose $\xi \neq 0$. Now $\xi \in \mathbb{F}_{q^m} - \mathbb{F}_q$, for if $\xi \in \mathbb{F}_q$, then $\alpha^{q^r} + \alpha^{q^{2r}} + \cdots + \alpha^{q^{rm}} = \alpha + \alpha^{q^r} + \cdots + \alpha^{q^{r(m-1)}} + m\xi$, contrary to $\xi \neq 0$ (since $p \nmid m$). Next, for any ν, $(\alpha - \nu)^{q^r} = \alpha^{q^r} - \nu^{q^r} = \alpha + \xi - \nu^{q^r} = (\alpha - \nu) - (\nu^{q^r} - \nu - \xi)$. The map $\nu \to \nu^{q^r} - \nu$ is easily seen to be a bijective map on $\mathbb{F}_{q^m} - \mathbb{F}_q$, so, for any $\xi \in \mathbb{F}_{q^m} - \mathbb{F}_q$, it is always possible to choose $\nu \in \mathbb{F}_{q^m} - \mathbb{F}_q$ satisfying $\nu^{q^r} - \nu - \xi = 0$. With this ν, $\alpha - \nu$ is the required fixed point.

We summarize in the following theorem.

THEOREM 4.1. *Under the action of M, $\mathbb{A}$ consists of consists of $(q^{r-1} - 1)/(q - 1)$ orbits of length 1 and*

$$\frac{1}{m}\left(\frac{q^{m(r-1)} - 1}{q^m - 1} - \frac{q^{r-1} + 1}{q - 1}\right)$$

orbits of length m.

5. Combining the actions of R and M

Suppose some $A(\alpha)$ is fixed by σ. By Theorem 4.1, we may assume that $\alpha^{q^r} = \alpha$ and $\alpha^q = \zeta\alpha + \xi$, and, by an argument similar to that at the beginning of the previous section, both $\zeta, \xi \in \mathbb{F}_q$. Thus, if $\zeta \neq 1$, $\alpha^{q^2} = \zeta\alpha^q + \xi = \zeta(\zeta\alpha + \xi) + \xi = \zeta^2\alpha + \zeta\xi + \xi$, and continuing in this way we obtain $\alpha = \alpha^{q^r} = \zeta^r\alpha + ((\zeta^r - 1)/(\zeta - 1))\xi$. We conclude that either $\zeta = 1$ or $\zeta \neq 1$ and $\zeta^r = 1$. If $\zeta = 1$, then $\alpha^q = \alpha + \xi$, and we note that $\xi \neq 0$ since $\alpha \notin \mathbb{F}_{q^m}$. As in Section 4, $\alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^r} = \alpha + \alpha^q + \cdots + \alpha^{q^{r-1}} + r\xi$ which forces $r\xi = 0$ and this is impossible (since $p \nmid r$).

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

Hence $\xi^r = 1, \xi \neq 1$ and so $r|q-1$. Conversely, let $r|q-1$. Then $r(q-1)|q^{rm}-1$ but $r(q-1) \nmid q^m - 1$ (by an argument similar to that in Section 3) and we may choose $\alpha \in \mathbb{S}$ of order $r(q-1)$ so $\alpha^{q-1} = \varepsilon$ has order r. Now $\alpha^q = \varepsilon\alpha$ and so $\alpha^q \in A(\alpha)$, and $(\zeta\alpha + \xi)^q = \zeta^q\alpha^q + \xi^q \in A(\alpha)$. Hence $A(\alpha)$ is fixed by σ. We have now proved the next result.

THEOREM 5.1. *There are affine sets fixed by σ if and only if $r \mid q-1$.*

6. Counting fixed points

We are now in position to apply the Cauchy-Frobenius counting theorem [5, Theorem 4.18] to the action of $\langle\sigma\rangle$ on $\mathbb{A}$. In all cases there are $(q^{m(r-1)}-1)/(q^m-1)$ affine sets fixed by the identity and $(q^{r-1}-1)/(q-1)$ sets fixed by M. In the case $r \mid q-1$ each of the $mr-1$ non-identity elements of order mr fixes $r-1$ sets and these $r-1$ sets are a subset of the set of $(q^{r-1}-1)/(q-1)$ sets fixed by M. If $r|q^m-1$ but $r \nmid q-1$, then each of the $r-1$ non-identity elements of order r fixes $r-1$ sets. If $r \nmid q^m-1$ there are no sets fixed by any element of order r. Define the function $N(q,m,r)$ to be

$$\frac{1}{mr}\left(\frac{q^{m(r-1)}-1}{q^m-1}+(rm-1)(r-1)+(m-1)\left(\frac{q^{r-1}-1}{q-1}-r+1\right)\right), \quad \text{if } r \mid q-1$$

$$\frac{1}{mr}\left(\frac{q^{m(r-1)}-1}{q^m-1}+(r-1)^2+(m-1)\left(\frac{q^{r-1}-1}{q-1}\right)\right), \quad \text{if } r \mid q^m-1,\ r \nmid q-1$$

$$\frac{1}{mr}\left(\frac{q^{m(r-1)}-1}{q^m-1}+(m-1)\left(\frac{q^{r-1}-1}{q-1}\right)\right), \quad \text{if } r \nmid q^m-1$$

Our main result is the following.

THEOREM 6.1. *The number of inequivalent G-codes is at most $N(q,m,r)$.*

The following table gives some values of $N(q,m,r)$.

q	m	r	$N(q,m,r)$
2	5	3	3
2	7	3	7
2	11	3	63
2	3	7	1791
4	5	3	71
4	7	3	783

q	m	r	$N(q,m,r)$
4	3	5	17765
4	3	7	51942291
8	3	5	8965437
5	7	3	3722
3	7	5	299003960
3	5	7	24308280100

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

References

[1] E. R. Berlekamp and O. Moreno, 'Extended double error correcting Goppa codes are cyclic', *IEEE Trans. Information Theory* **IT–19** (1973), 817–818.

[2] C.-L. Chen, 'Equivalent irreducible Goppa codes', *IEEE Trans. Information Theory* **IT–24** (1978), 766–769.

[3] M. Elia, G. Taricco and V. Viterbo, 'On the classification of binary Goppa codes', presented at *ISITA, Honolulu, Nov. 2000.*

[4] J. K. Gibson, 'Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem', in: *Advances in Cryptology — EUROCRYPT 91 (Brighton 1991)*, Lecture Notes in Comput. Sci. 547 (Springer, Berlin, 1991) pp. 517–521.

[5] I. M. Isaacs, *Algebra: A graduate text* (Brooks/Cole, Pacific Grove, CA, 1994).

[6] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications* (Cambridge Univ. Press, Cambridge, 1994).

[7] O. Moreno, 'Symmetries of binary Goppa codes', *IEEE Trans. Information Theory* **IT–25** (1979), *609–612.*

[8] V. S. Pless, W. C. Huffman and R. A. Brualdi (eds.), *Handbook of coding theory* (North-Holland, Amsterdam, 1998).

Department of Mathematics
University College Cork
Ireland
e-mail: fitzpat@ucc.ie

Department of Mathematics
Mzuzu University
Malawi
e-mail: mzuzu_jar@oceanfree.net

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949

Downloaded from https://www.cambridge.org/core. IP address: 133.200.211.161, on 29 Mar 2021 at 13:40:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S1446788700002949