Choosing elements from finite fields

Michael Vaughan-Lee

November 2012

1 Introduction

Graham Higman wrote two immensely important and influential papers on enumerating p-groups in the late 1950s. The papers were entitled *Enumerating p-groups* I and II, and were published in the Proceedings of the London Mathematical Society in 1960 (see [1] and [2]). In these two papers Higman proved that for any given n, the function $f(p^n)$ enumerating the number of p-groups of order p^n is bounded by a polynomial in p, and he formulated his famous PORC conjecture concerning the form of the function $f(p^n)$. He conjectured that for each n there is an integer N (depending on n) such that for p in a fixed residue class modulo N the function $f(p^n)$ is a polynomial in p. For example, for $p \geq 5$ the number of groups of order p^6 is

$$3p^2 + 39p + 344 + 24 \gcd(p-1, 3) + 11 \gcd(p-1, 4) + 2 \gcd(p-1, 5).$$

(See [3].) So for $p \geq 5$, $f(p^6)$ is one of 8 polynomials in p, with the choice of polynomial depending on the residue class of p modulo 60. The number of groups of order p^6 is **P**olynomial **O**n **R**esidue **C**lasses. As evidence in support of his PORC conjecture Higman proved that, for any given n, the function enumerating the number of p-class 2 groups of order p^n is a PORC function of p. He obtained this result as a corollary to a very general theorem about vector spaces acted on by the general linear group. As another corollary to this general theorem, he also proved that for any given n the function enumerating the number of algebras of dimension n over the field of q elements is a PORC function of q. A key step in Higman's proof of these results is Theorem 2.2.2 from [2].

Theorem 1 (Higman [2]) *The number of ways of choosing a finite number of elements from $\mathbb{F}_{q^n}$ subject to a finite number of monomial equations and inequalities between them and their conjugates over $\mathbb{F}_q$, considered as a function of q, is PORC.*

The statement of this theorem probably requires some explanation! Here we are choosing elements $x_1, x_2, \ldots, x_k$ (say) from the finite field $\mathbb{F}_{q^n}$ (where q is a prime power) subject to a finite set of equations and non-equations of the form

$$x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} = 1$$

and
$$x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} \neq 1,$$

where $n_1, n_2, \ldots, n_k$ are integer polynomials in the Frobenius automorphism $x \mapsto x^q$ of $\mathbb{F}_{q^n}$. Higman calls these equations and non-equations *monomial*. For example, suppose we want to choose $x_1, x_2 \in \mathbb{F}_{q^n}$ such that x_1 is the root of an irreducible quadratic over $\mathbb{F}_q$ and such that x_2^2 is the product of the roots of this quadratic. Then we require that x_1 and x_2 satisfy

$$x_1^{q^2-1} = 1, \ x_1^{q-1} \neq 1, \ x_1^{q+1} x_2^{-2} = 1. \tag{1}$$

The equation $x_1^{q^2-1} = 1$ guarantees that x_1 is the root of a quadratic over $\mathbb{F}_q$, and the non-equation $x_1^{q-1} \neq 1$ guarantees that $x_1 \notin \mathbb{F}_q$ so that the quadratic is irreducible. The other root of the quadratic is then x_1^q, so the last equation guarantees that x_2^2 is the product of the roots. To make sure that $x_1, x_2 \in \mathbb{F}_{q^n}$, we also require that $x_1^{q^n-1} = 1$, $x_2^{q^n-1} = 1$. Higman's theorem is that the function enumerating the number of solutions to (1) in $\mathbb{F}_{q^n}$ is a PORC function of q.

In this note we give very precise information about the exact form of the PORC functions needed to enumerate the number of solutions to a set of monomial equations.

Higman's proof of his Theorem 2.2.2 involves five pages of homological algebra. A shorter more elementary proof can be found in [4]. The proof in [4] shows that one way to calculate the number of solutions to a set of monomial equations is to write the equations as the rows of a matrix. So we represent the equations

$$x_1^{q^2-1} = 1, \ x_1^{q+1} x_2^{-2} = 1, \ x_1^{q^n-1} = 1, \ x_2^{q^n-1} = 1$$

by the matrix

$$\begin{bmatrix} q^2 - 1 & 0 \\ q + 1 & -2 \\ q^n - 1 & 0 \\ 0 & q^n - 1 \end{bmatrix}.$$

For any given value of q the matrix becomes an integer matrix, and it is shown in [4] that the number of solutions is the product of the elementary divisors in the Smith normal form of this integer matrix. To obtain the number of solutions to (1) in $\mathbb{F}_{q^n}$ we subtract the number of solutions to the equations

$$x_1^{q-1} = 1, \ x_1^{q+1} x_2^{-2} = 1, \ x_1^{q^n-1} = 1, \ x_2^{q^n-1} = 1.$$

The number of solutions to these equations is just the product of the elementary divisors in the Smith normal form of the matrix

$$\begin{bmatrix} q - 1 & 0 \\ q + 1 & -2 \\ q^n - 1 & 0 \\ 0 & q^n - 1 \end{bmatrix}.$$

(In [4] q is assumed to be prime, but the proof is still valid when q is a prime power.)

Matrices used in this way to represent a set of monomial equations have entries which are integer polynomials in q. The columns correspond to the unknowns we are solving for, and since there will always be rows $(q^n-1, 0, 0, \ldots, 0)$, $(0, q^n-1, 0, \ldots, 0)$, $\ldots, (0, \ldots, 0, q^n-1)$ corresponding the requirement that the unknowns are elements in $\mathbb{F}_{q^n}$, it follows that the rank of one of these matrices is the number of columns. So the product of the elementary divisors in the Smith normal form of one of these matrices is the greatest common divisor of the $k \times k$ minors, where k is the number of columns. These $k \times k$ minors are integer polynomials in q, and it is proved in [4] that the greatest common divisor of a set of integer polynomials in q is a PORC function of q. There is some ambiguity about what "the greatest common divisor of a set of polynomials" means here. Suppose we have some integer polynomials $f_1(q), f_2(q), \ldots, f_s(q)$. For any given value of q these polynomials evaluate to integers, and by "greatest common divisor of the polynomials" we actually mean "greatest common divisor of the values of the polynomials at q". It is this integer valued function of q which we claim is PORC, and it turns out that we can be quite precise about the form that this PORC function takes.

Theorem 2 *The greatest common divisor of a set of integer polynomials in q can be expressed in the form df where f is an integer polynomial in q and where*

$$d = \alpha + \sum_{i=1}^{r} \alpha_i \gcd(q - n_i, m_i)$$

for some rational numbers $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r$, some integers $m_1, m_2, \ldots, m_r$ with $m_i > 1$ for all i, and some integers $n_1, n_2, \ldots, n_r$ with $0 < n_i < m_i$ for all i.

Corollary 3 *The number of ways of choosing a finite number of elements from $\mathbb{F}_{q^n}$ subject to a finite number of monomial equations and inequalities between them and their conjugates over $\mathbb{F}_q$ can be expressed as a linear combination of terms of the form df, where f and d are as described in Theorem 2.*

2 Choosing field elements

To make this note self contained, we give a proof here that we can use a matrix to represent a set of monomial equations over a finite field, and that the number of solutions to the equations is the product of the elementary divisors in the Smith normal form of the matrix.

So suppose we have a set of monomial equations in unknowns $x_1, x_2, \ldots, x_k$, and suppose that we want to find the number of solutions to these equations in the field $\mathbb{F}_{q^n}$. We represent the equations in a matrix A with k columns, with a row $(n_1, n_2, \ldots, n_k)$ for each monomial equation $x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} = 1$. We also add in rows

$$(q^n - 1, 0, 0, \ldots, 0), \ (0, q^n - 1, 0, \ldots, 0), \ \ldots, \ (0, 0, \ldots, 0, q^n - 1)$$

corresponding to the requirement that $x_1, x_2, \ldots, x_k \in \mathbb{F}_{q^n}$. Note that the entries in the matrix A are integer polynomials in q. We now take a particular value for q so that the matrix becomes a matrix with integer entries.

Let ω be a primitive element in $\mathbb{F}_{q^n}$, and write $x_i = \omega^{m_i}$ for $i = 1, 2, \ldots, k$, taking the exponents m_i as elements in $\mathbb{Z}_{q^n-1}$. Then a row $(\beta_1, \beta_2, \ldots, \beta_k)$ in the matrix A corresponds to a relation $\beta_1 m_1 + \beta_2 m_2 + \ldots + \beta_k m_k = 0$ which we require the exponents m_i to satisfy. The matrix A can be reduced to Smith normal form over $\mathbb{Z}$ by elementary row and column operations. As we apply these operations, the relations encoded in the matrix change. But we show that at each step the number of solutions to the relations stays constant.

This is clear for elementary row operations, since an elementary row operation replaces the relations by an equivalent set of relations. So we need to consider the effect of elementary column operations. We can consider the k-tuples $(m_1, m_2, \ldots, m_k)$ as elements in the additive group $G = \mathbb{Z}_{q^n-1} \times \mathbb{Z}_{q^n-1} \times \ldots \times \mathbb{Z}_{q^n-1}$. Let A be one of these relation matrices, and let B be the matrix obtained from A after applying an elementary column operation. For each such operation we define an automorphism σ of G with the property that $g \in G$ satisfies the relations given by the rows of A if and only if $g\sigma$ satisfies the relations given by the rows of B. This shows that the number of elements in G satisfying the relations given by A is the same as the number of elements in G satisfying the relations given by B. If the elementary column operation swaps two columns of A then we let σ be the automorphism which swaps the corresponding entries in $(m_1, m_2, \ldots, m_k)$, and if the elementary column operation multiplies a column by -1 we let σ be the automorphism which multiplies the corresponding entry in $(m_1, m_2, \ldots, m_k)$ by -1. Finally, if the elementary column operation subtracts α times column j from column i, then we let σ be the automorphism which leaves all the entries in $(m_1, m_2, \ldots, m_k)$ fixed except for the j-th entry, which it replaces by $m_j + \alpha m_i$.

The argument above shows that the number of $g \in G$ satisfying the original set of relations given by the rows of A is the same as the number of $g \in G$ satisfying the relations given by the Smith normal form A. If the elementary divisors in the Smith normal form are $d_1, d_2, \ldots, d_k$, then $(m_1, m_2, \ldots, m_k)$ is a solution to these equations if and only if

$$d_1 m_1 = d_2 m_2 = \ldots = d_k m_k = 0.$$

Provided we can show that $d_i | q^n - 1$ for all i, this shows that the number of solutions is $d_1 d_2 \ldots d_k$, as claimed.

If A is one of these relation matrices with k columns, then the rows of A are elements in the free $\mathbb{Z}$-module $F = \mathbb{Z}^k$. We let $R(A)$ denote the $\mathbb{Z}$-submodule of F generated by the rows of A. Our claim that $d_i | q^n - 1$ for all i amounts to the claim that $(q^n - 1)F \leq R(S)$, where S is the Smith normal form of our initial relation matrix. The Smith normal form is obtained from the initial matrix by a sequence of elementary row and column operations, and we show that $(q^n - 1)F \leq R(B)$ for all the matrices B generated in this sequence.

Let A be the starting matrix. Then it contains rows

$$(q^n - 1, 0, 0, \ldots, 0), (0, q^n - 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, q^n - 1),$$

4

so it is clear that $(q^n - 1)F \leq R(A)$. Suppose that at some intermediate stage in the reduction of A to Smith normal form we have two matrices B and C, where C is obtained from B by an elementary row operation or an elementary column operation. We assume by induction that $(q^n - 1)F \leq R(B)$, and we show that this implies that $(q^n - 1)F \leq R(C)$. This is clear if C is obtained from B by an elementary row operation, since then $R(B) = R(C)$. So consider the case when C is obtained from B by an elementary column operation. This column operation corresponds to an automorphism σ of F, and if r is a row of B then the corresponding row of C is $r\sigma$. So $R(C) = R(B)\sigma$, and the fact that $(q^n - 1)F$ is a characteristic submodule of F implies that $(q^n - 1)F \leq R(C)$.

This completes the proof that the number of solutions to the relations given by the rows of the matrix is equal to the product of the elementary divisors in the Smith normal form. As mentioned in the introduction, the product of the elementary divisors in the Smith normal form of an integer matrix with k columns and rank k is the greatest common divisor of the $k \times k$ minors. In the situation we are concerned with, these minors are integer polynomials in q. So the number of solutions to our monomial equations is the greatest common divisor of a set of integer polynomials in q. More precisely, we have a set of integer polynomials in q, and for any given value of q the number of solutions to our monomial equations is the greatest common divisor over $\mathbb{Z}$ of the values of these polynomials at q.

3   Proof of Theorem 2

Let $f_1(q)$, $f_2(q)$, ..., $f_s(q)$ be a set of integer polynomials in q. We want to compute the function whose value at q is the greatest common divisor of the integers $f_1(q)$, $f_2(q)$, ..., $f_s(q)$. In this section there is no requirement that q be a prime power, and to make this clear we define a function $h : \mathbb{Z} \to \mathbb{Z}$ by setting

$$h(x) = \gcd(f_1(x), f_2(x), \ldots, f_s(x)) \text{ for } x \in \mathbb{Z}.$$

It is the function h we want to compute. As mentioned above, there is some ambiguity about what we mean by "the greatest common divisor of $f_1(x)$, $f_2(x)$, ..., $f_s(x)$". We now exploit this ambiguity, and treat x as an indeterminate and treat $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ as elements of the Euclidean domain $\mathbb{Q}[x]$.

We can use the Euclidean algorithm to compute the greatest common divisor $f(x)$ of $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ in $\mathbb{Q}[x]$ and we can take $f(x)$ to be a primitive polynomial in $\mathbb{Z}[x]$. We then obtain polynomials $g_1, g_2, \ldots, g_s \in \mathbb{Q}[x]$ such that

$$f_1 g_1 + f_2 g_2 + \ldots + f_s g_s = f.$$

Let m be the least common multiple of the denominators of the coefficients in $g_1, g_2, \ldots, g_s$. Then for any given value of x in $\mathbb{Z}$, the greatest common divisor of the integers $f_1(x)$, $f_2(x)$, ..., $f_n(x)$ is $df(x)$ for some d dividing m. Furthermore, as a function of x, the value of d at x depends only on the residue class of x modulo m.

We show that we can express $d(x)$ in the form

$$\alpha + \sum_{i=1}^{r} \alpha_i \gcd(x - n_i, m_i)$$

described in the statement of Theorem 2. Furthermore we show that we can take the integers m_i to be of the form $\frac{m}{d_i}$ for some square free divisors d_i of m with $d_i < m$. This shows that $h(x) = d(x)f(x)$ has the form described in Theorem 2.

If $m = 1$ then $d = 1$ for all x, and we are done. So suppose that $m > 1$ and let S be the set of prime factors of m. For each subset $T \subset S$ let

$$d_T = \prod_{p \in T} p,$$

and consider the function $k : \mathbb{Z} \to \mathbb{Z}$ defined by

$$k(x) = \sum_{T \subset S} (-1)^{|T|} \gcd(x, \frac{m}{d_T}).$$

Clearly the value of k at any given value of x depends only on the residue class of x modulo m. First consider the case when $x = m$.

$$k(m) = \sum_{T \subset S} (-1)^{|T|} \frac{m}{d_T} = m \prod_{p \in S} (1 - \frac{1}{p}) \neq 0.$$

Next suppose that $1 \leq x < m$. Then there is at least one $p \in S$ with the property that the power of p dividing x is less than the power of p dividing m. Pick one such p and let $U = S \backslash \{p\}$. Then

$$k(x) = \sum_{T \subset U} (-1)^{|T|} \left(\gcd(x, \frac{m}{d_T}) - \gcd(x, \frac{m}{pd_T}) \right) = 0,$$

since $\gcd(x, \frac{m}{d_T}) = \gcd(x, \frac{m}{pd_T})$ for all $T \subset U$. So if we let $c = k(m)$ then $\frac{1}{c}k(x)$ takes values $0, 0, \ldots, 0, 1$ as x takes values $1, 2, \ldots, m$ modulo m. It follows that if $0 < a < m$ then $\frac{1}{c}k(x-a)$ takes values $0, \ldots, 0, 1, 0, \ldots, 0$ as x takes values $1, 2, \ldots, m$ modulo m (with the 1 in the ath place). So we can express $d(x)$ as a rational linear combination of the functions $k(x - a)$ for $0 \leq a < m$. This implies that we can express $d(x)$ as a rational linear combination of functions of the form $\gcd(x - n_i, m_i)$ where $m_i = \frac{m}{d_T}$ for some $T \subset S$. If $m_i = 1$ then we can replace $\gcd(x - n_i, m_i)$ by the constant 1. Also, we can assume $0 \leq n_i < m_i$. Finally, using the fact that

$$\sum_{a=0}^{m_i-1} \gcd(x - a, m_i)$$

is a constant function, we can assume that $0 < n_i < m_i$, provided we add a constant term into our expression for $d(x)$. This completes the proof of Theorem 2. Note that the proof shows that we can assume that the denominators of the rational coefficients which appear in the expression for $d(x)$ divide the constant $k(m)$.

6

References

[1] G. Higman, *Enumerating p-groups. I: Inequalities*, Proc. London Math. Soc. **(3) 10** (1960), 24–30.

[2] G. Higman, *Enumerating p-groups. II: Problems whose solution is PORC*, Proc. London Math. Soc. **(3) 10** (1960), 566–582.

[3] M.F. Newman, E.A. O'Brien, and M.R. Vaughan-Lee, *Groups and nilpotent Lie rings whose order is the sixth power of a prime*, J. Algebra **278** (2004), 383–401.

[4] Michael Vaughan-Lee, *On Graham Higman's famous PORC paper*, Internat. J. Group Theory **1** (2012), 65–79.