DEPENDENT SETS OF CONSTANT WEIGHT VECTORS IN $GF(q)$

NEIL J. CALKIN

Abstract. We determine lower bounds for the number of random vectors in $GF(q)$, chosen uniformly from vectors having k non-zero co-ordinates, needed to obtain a dependent set over $GF(q)$.

1. Introduction

In this paper we determine lower bounds for the number of random vectors in $GF(q)$ of weight k, i.e. having k non-zero entries, needed to obtain a dependent set of vectors with probability 1.

We denote by $S_{n,k}$ the set of vectors having k non-zero entries. If we choose a random sequence $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_m$ uniformly from $S_{n,k}$, how large must m be for these vectors to be linearly dependent (over $GF(q)$)?

In [2] it was shown that when $q = 2$ at least $\beta_k n$ vectors are necessary, where for large values of k, $\beta_k \sim 1 - \frac{e^{-k}}{\log 2}$. In this paper we show that similar techniques can be used for a general finite field $GF(q)$. In related work, Balakin, Kolchin and Khokhlov have obtained essentially equivalent results for the binary case [1] and for the case where q is prime [3, 4].

For brevity, we shall follow the notation of [2]. Let $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_m, \ldots$ be chosen uniformly and independently at random from the set of vectors of weight k in $GF(q)$.

Let the random variable $s = s_m$ be the co-rank of the vectors $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_m$, that is, m minus the rank. Then q^s is equal to the number of distinct solutions of

$$c_1\underline{u}_1 + c_2\underline{u}_2 + \cdots + c_m\underline{u}_m = \underline{0}$$

with $\underline{c} = (c_1, c_2, \ldots c_m) \in GF(q)^m$. We make use of a suitable Markov chain to determine the threshold function $m(n)$ for $E(q^s)$ to tend to infinity: then if $E(q^s)$ is close to 1, the vectors are almost surely independent.

Define

$$\underline{x}_0 = \underline{0}, \quad \text{and} \quad \underline{x}_l = \underline{x}_{l-1} + \underline{u}_l$$

so that $\underline{x}_l$ and $\underline{x}_{l-1}$ differ by a random vector of weight k. Let X_l be the weight of $\underline{x}_l$. Then $X_0, X_1, \ldots, X_m$, is a Markov chain with states $\{0, 1, \ldots, n\}$. The transition matrix A for this chain, with $A = \{a_{ij}\}$, where a_{ij} is the probability of moving from state j to state i is given by

$$a_{ij} = \sum_{t=0}^{k} \frac{1}{\binom{n}{k}} \binom{j}{t} \binom{j-t}{j-2t-i+k} \binom{n-j}{i-j-t} (q-2)^{j-2t-i+k} (q-1)^{i-j-t-k}.$$

1991 *Mathematics Subject Classification.* 05C80.

Theorem 1. *The eigenvalues λ_i and corresponding eigenvectors $\underline{e}_i$ for A, $i = 0, 1, \ldots, n$, are given by*

$$\lambda_i = \sum_{t=0}^{k} (-1)^{k+t} \frac{\binom{i}{t}\binom{n-i}{k-t}(q-1)^t}{\binom{n}{k}(q-1)^k} \tag{1}$$

and the jth component of $\underline{e}_i$ is given by

$$\underline{e}_i[j] = \sum_{t=0}^{j} (-1)^{t+j} \binom{i}{t}\binom{n-t}{j-t} q^t.$$

Proof: Let U be the matrix of eigenvectors, that is the matrix whose ijth entry is

$$U_{i,j} = \underline{e}_j[i] = \sum_{t=0}^{i} (-1)^{t+i} \binom{j}{t}\binom{n-t}{i-t} q^t$$

and let V be the matrix in reverse order, that is $V_{i,j} = U_{n-i,n-j}$. We shall show that $UV = q^n I$, which implies that U and V are both invertible, and hence that the eigenvectors claimed above are linearly independent.

Indeed, consider the general term

$$(UV)_{i,j} = \sum_l U_{i,l} V_{l,j} = \sum_l \underline{e}_l[i] \underline{e}_{n-j}[n-l]$$

$$= \sum_{l,s,t} (-1)^{s+i} \binom{l}{s}\binom{n-s}{i-s} q^s (-1)^{t+n+l} \binom{n-j}{t}\binom{n-t}{l} q^t.$$

Multiplying this by x^i and summing over i, we obtain

$$\sum_{l,s,t} \binom{l}{s} q^s x^s (1-x)^{n-s} (-1)^{t+n+l} \binom{n-j}{t}\binom{n-t}{l} q^t$$

$$= \sum_{l,t} (-1)^{t+n+l} (1-x+qx)^l (1-x)^{n-l} \binom{n-j}{t}\binom{n-t}{l} q^t$$

$$= \sum_t q^{n-t} x^{n-t} (1-x)^t \binom{n-j}{t} q^t$$

$$= q^n x^j$$

i.e. $(UV)_{i,j} = q^n$ if $i = j$, and 0 otherwise, proving that $UV = q^n I$.

The proof that the eigenvectors are indeed eigenvectors follows by similar methods. Since this is just a case of checking simple binomial identites, and the method of proof is rather similar to that of [2] we omit the details. □

We can now determine the expectation $E(q^s)$.

Theorem 2.

$$E(q^s) = \sum_{j=0}^{n} \frac{1}{q^n} \binom{n}{j} (1 + (q-1)\lambda_i)^m (q-1)^{n-i}$$

Proof: Observe that the probability that a set of vectors $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_t$ sum to $\underline{0}$ is exactly the 00th coefficient of A^t. Now, for any fixed non-zero $c_1, c_2, \ldots c_t \in GF(q)$, the probability that $c_1\underline{u}_1 + c_2\underline{u}_2 + \ldots c_t\underline{u}_t = \underline{0}$ is equal to the probability that $\underline{u}_1 + \underline{u}_2 + \cdots + \underline{u}_t = \underline{0}$ since the vectors $c_i\underline{u}_i$ are also uniformly distributed with weight k (this, of course, depends upon the fact that $GF(q)$ is a field, and is the point at which this work fails to apply to powers of rings).

Hence the expected number of solutions $c_1, c_2, \ldots, c_m$, (allowing some or all of the c_i to be 0) to the equation $c_1\underline{u}_1 + c_2\underline{u}_2 + \ldots c_t\underline{u}_m = \underline{0}$ is the 00th coefficient of

$$\sum_t^m (q-1)^t A^t \binom{m}{t} = (I + (q-1)A)^m = \frac{1}{q^n} U(I + (q-1)\Lambda)^m V,$$

where Λ is the $(n+1) \times (n+1)$ diagonal matrix of eigenvalues, and U is the matrix whose columns are the eigenvectors, and $UV = q^n I$ as above.

Now, since the 00th coefficient of $\frac{1}{q^n} U(I + (q-1)\Lambda)^m V$ is

$$\frac{1}{q^n} \sum_i \underline{e}_i[0](1 + (q-1)\lambda_i)^m \underline{e}_n[n-i]$$

$$E(q^s) = \sum_{i=0}^{n} \frac{1}{q^n} \binom{n}{i} (1 + (q-1)\lambda_i)^m (q-1)^{n-i}.$$

□

We now consider the asymptotic behaviour of the sum.

Theorem 3. *For any $q, k \geq 3$ there is a constant β_k so that*
a) If $\beta < \beta_k$ and $m = m(n) < \beta n$ then $E(q^s) \to 1$ as $n \to \infty$.
b) If $\beta > \beta_k$ and $m = m(n) > \beta n$ then $E(q^s) \to \infty$ as $n \to \infty$.
Furthermore, $1 - \beta_k \sim \frac{(q-1)e^{-k}}{\log q}$ as $k \to \infty$.

Proof: First, observe that the tails of the sum contribute $o(1)$ to the sum. Moreover, it is easy to see that unless i/n is very close to $(q-1)/q$ then $\lambda_i \sim (1 - qi/(q-1)n)^k$: it follows from this and some straightforward but tedious estimates that for sufficiently small δ, the portion of the sum when i/n is in the range $((q-1)/q - \delta, ((q-1)/q + \delta)$ is asymptotic to 1, provided that m is not too big, say $m = O(n)$. Since this is certainly the case, we can now concentrate on the remainder of the sum. Let $\sum'$ denote the remainder of the sum. Then writing $\alpha = i/n$ and $\beta = m/n$, we see that if every remaining term is exponentially small in n, then the sum is exponentially small, since there are only n terms: if there is a term which is exponentially large, then the sum is exponentially large.

Now define

$$f(\alpha, \beta) = -\log q + (1-\alpha)\log(q-1) - \alpha\log(\alpha) - (1-\alpha)\log(1-\alpha)$$
$$+\beta \log(1 + (q-1)(\frac{q\alpha - 1}{q-1})^k).$$

Then for large n, the term in the sum corresponding to i is about $\exp(nf(\frac{i}{n}, \frac{m}{n})$: hence if there exists an $\epsilon > 0$ so that for every

$$\alpha \in (\delta, (q-1)/q - \delta) \cup ((q-1)/q + \delta, 1 - \delta),$$

$f(\alpha, m/n)$ is less than $-\epsilon$, then $\sum' < ne^{-\epsilon n}$ term is exponentially small, and if there is a value of α for which $f(\alpha, m/n) > \epsilon$, then there is an exponentially large term, and $\sum' > e^{\epsilon n}$.

Let $\beta_{k,q} = \beta_k$ be the least value in $(0,1)$ for which there exists an $\alpha_k \in (0,1)$ with $f(\alpha_k, \beta_k) = 0$, then $m = n\beta_k$ is the threshold function for $E(q^s) \to \infty$, that is,

$$\text{if } \beta < \beta_k \text{ and } m < \beta n \text{ then } E(q^s) \to 1 \text{ and}$$

$$\text{if } \beta > \beta_k \text{ and } m > \beta n \text{ then } E(q^s) \to \infty.$$

We consider the asypmtotics of α_k and β_k as q and k tend to ∞. First, we shall reparametrize f in $\theta = \frac{q\alpha-1}{q-1}$, so that

$$f(\alpha,\beta) = f(1 - \tfrac{(1-\theta)(q-1)}{q}, \beta)$$

$$= -\frac{(q-1)(1-\theta)\log(1-\theta)}{q} - \frac{(1+(q-1)\theta)\log(1+(q-1)\theta)}{q} + \beta\log(1+q\theta^k)$$

and

$$\frac{\partial f}{\partial \theta} = -\frac{q-1}{q}\log\left(\frac{(q-1)\theta+1}{1-\theta}\right) + \frac{\beta k(q-1)\theta^{k-1}}{(1+(q-1)\theta^k)}.$$

Observe that when $\theta = 0$, both f and f' are 0. This corresponds to the portion of the sum around $i = n/q$. Moreover, for k and q sufficiently large, there are no other roots of $f = f' = 0$ with θ in the interval $(-1/(q-1), 1/(q-1))$. Continuing to bootstrap, we see by examining the equation for f', and using $\beta_k \le 1$, that $k(q-1)\theta_k^{k-1} \not\to 0$. This implies that there is a constant c so that for k, q sufficiently large, $\theta_k > cq^{-1/k}$. Thus $\log((q-1)\theta+1)$ is about $\log((q-1)\theta) > (1-1/k)\log(q-1) + \log(c)$. By considering the expression for f, and again using the fact that $\beta_k \le 1$, we see that as $q, k \to \infty$, $q\theta_k^k \to \infty$. Thus, if $k >> \log q$, θ_k must be close to 1. It is then simple to expand the equations around $\theta = 1$ and $\beta = 1$ to obtain that for any fixed q, as $k \to \infty$,

$$1 - \beta_k \sim \frac{(q-1)e^{-k}}{\log q}$$

and

$$1 - \alpha_k \sim (q-1)e^{-k}.$$

□

Corollary 1. *For any fixed k, q, if $\beta < \beta_k$ and $m < \beta n$, then as $n \to \infty$, the probability that the vectors $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_m$ are linearly dependent tends to 0.*

As a final observation, we point out that since the eigenvectors $\underline{e}_i$ do not depend upon k, the transition matrices corresponding to vectors of weight k and weight k' commute: this is not surprising, since this corresponds to the fact that adding a random vectors of weight k and k' doesn't depend on the order in which they are added. As a corollary, however, it means that any distribution of vectors depending only on weight (that is, vectors of the same weight are equiprobable) can be handled by the methods above. In particular, the model used by Kolchin and Khokhlov, which is essentially to let each vector $\underline{u}_i$ be the sum of k independent vectors of weight 1, corresponds to taking the transition matrix for 1, and raising it to the kth power: in this case, the eigenvalues obtained are exactly equal to

$$\left(1 - \frac{qi}{(q-1)n}\right)^k,$$

and their results for finite fields of prime order follow immediately.

References

[1] G. V. Balakin, V. F. Kolchin and V. I. Khokhlov, *Hypercycles in a random hypergraph*, Discrete Math. Appl., 2 (1992), pp. 563–570.

[2] Neil J. Calkin, *Dependent sets of constant weight binary vectors*, Combinatorics, Probability and Computing. To appear.

[3] V. F. Kolchin, *Random graphs and systems of linear equations in finite fields*, Random Structures and Algorithms, 5 (1994), pp. 135–146. In Russian.

[4] V. F. Kolchin and V. I. Khokhlov, *A threshold effect for systems of random equations of a special form*, Discrete Mathematics and Applications, 5 (1995), pp. 425–436.

School Of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332
E-mail address: calkin@math.gatech.edu