Electronic Journal of Linear Algebra

Volume 20 *ELA Volume 20 (2010)* Article 1

2010

Spaces of constant rank matrices over GF(2)

Nigel Boston
boston@math.wisc.edu

Recommended Citation
Boston, Nigel. (2010), "Spaces of constant rank matrices over GF(2)", *Electronic Journal of Linear Algebra*, Volume 20.
DOI: https://doi.org/10.13001/1081-3810.1354

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 1-5, January 2010

ELA
http://math.technion.ac.il/iic/ela

SPACES OF CONSTANT RANK MATRICES OVER $GF(2)$*

NIGEL BOSTON†

Abstract. For each n, we consider whether there exists an $(n+1)$-dimensional space of n by n matrices over $GF(2)$ in which each nonzero matrix has rank $n-1$. Examples are given for $n = 3, 4$, and 5, together with evidence for the conjecture that none exist for $n > 8$.

Key words. Constant rank, Matrices, Heuristics.

AMS subject classifications. 15A03, 15-04.

1. Introduction. There has been much interest [5], [7, Chapter 16D] in spaces of matrices in which every nonzero matrix has the same rank. We call this a space of matrices of constant rank. Often there is some algebraic construction behind the examples - for instance, taking a basis for $GF(q^n)$ over $GF(q)$ yields an n-dimensional space of n by n matrices over $GF(q)$ of constant rank n.

We focus on spaces of n by n matrices of constant rank $n-1$, and ask how large their dimensions can be. In [5], it was shown that for real matrices, the maximal dimension is $\max\{\rho(n-1), \rho(n), \rho(n+1)\}$, where ρ is the Hurwitz-Radon function, except for $n = 3$ and 7 when the maximal dimension is 3 and 7, respectively. As regards matrices over a general field F, it was shown in [2] that if $|F| \geq n$, then this maximal dimension is at most n. The question then arises as to whether for smaller fields F there can be such spaces of larger dimension, $n+1$.

As noted below, $GF(2)$ has the unusual property that there are about twice as many n by n matrices of rank $n-1$ over it as there are matrices of rank n, and so interest has focused on this case. By the above, if $n < 3$, then the maximal dimension is at most n. In [1], Beasley found a couple of spaces of n by n matrices of constant rank $n-1$ and dimension $n+1$ for $n = 3$. He conjectured that no examples exist for $n > 3$, but this author found, by search using the computer algebra system MAGMA [3], examples for $n = 4$ and $n = 5$. The temptation now is to conjecture that examples exist for all n, but as we shall see, heuristics do not support such a claim.

*Received by the editors September 11, 2009. Accepted for publication December 8, 2009. Handling Editor: Bryan L. Shader.

†Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA (boston@math.wisc.edu). Supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006 and Stokes Professorship award, Science Foundation Ireland Grant 07/SK/I1252b.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 1-5, January 2010

ELA
http://math.technion.ac.il/iic/ela

2. Low dimensional examples. This section exhibits spaces of n by n matrices of constant rank $n-1$ and dimension $n+1$ for $n = 3, 4$, and 5. For $n = 3$, Beasley [1] found some examples. An exhaustive MAGMA search shows that there are exactly 1176 such spaces. Under conjugation by $GL(3, 2)$, these fall into 12 orbits. A basis for a representative of each orbit is given:

Orbit length 168: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$

Orbit length 168: $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$

Orbit length 168: $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$

Orbit length 168: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$

Orbit length 84: $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$

Orbit length 84: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$

Orbit length 84: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$

Orbit length 84: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$

Orbit length 56: $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$

Orbit length 42: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 1-5, January 2010

ELA
http://math.technion.ac.il/iic/ela

$$\text{Orbit length 42: } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$\text{Orbit length 28: } \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

An example of a 5-dimensional space of 4 by 4 matrices of constant rank 3 is given by the span of the following matrices:

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

An example of a 6-dimensional space of 5 by 5 matrices of constant rank 4 is given by the span of the following matrices:

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

These were discovered by careful search using the computer algebra system, MAGMA [3].

3. Heuristics. Let $C(n, r, q)$ denote the number of n by n matrices of rank r over $GF(q)$. Landsberg [6] (later refined by Buckheister [4] to count matrices with a given rank and trace) showed that

$$C(n, r, q) = q^{r(r-1)/2} \prod_{i=1}^{r} (q^{n-i+1} - 1)^2 / (q^i - 1).$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 1-5, January 2010

As $n \to \infty$, the probability that an n by n matrix over $GF(q)$ has rank $n-r$, i.e., the ratio of $C(n, n-r, q)$ to the total number of matrices q^{n^2}, tends to a limit $K(r, q)$, where for instance $K(0, 2) = 0.2888,\ K(1, 2) = 0.5776$, (which is the basis for the statement above that an n by n matrix over $GF(2)$ is twice as likely to have rank $n-1$ as rank n), $K(2, 2) = 0.1284,\ K(3, 2) = 0.0052, \ldots$ Since we will make great use of $K(1, 2)$ in this paper, note that to 20 decimal places $K(1, 2) = 0.57757619017320484256$.

Our heuristic claims that, in the absence of any other algebraic structure, the probability that each matrix in a space of n by n matrices has rank $n-r$ should be independently approximated by $K(r, q)$. Let $N(n, r, q, d)$ denote the number of ordered d-tuples of n by n matrices over $GF(q)$ for which all nontrivial linear combinations have rank $n-r$. By the above heuristic, this should be about $K(r, q)^{q^d-1}$ multiplied by the total number of ordered d-tuples, namely q^{dn^2}, i.e.,

$$N(n, r, q, d) \approx K(r, q)^{q^d-1} q^{dn^2}.$$

To test our heuristic, let S_n be the set of all n by n matrices over $GF(2)$ of rank $n-1$. We seek the probability that, given $M_1, M_2 \in S_n,\ M_1 + M_2$ also lies in S_n. Exhaustive computation shows that it equals $(2/3)^2 = 0.4444, (85/147)^2 = 0.5782, (2722/4725)^2 = 0.5761, (174751/302715)^2 = 0.5773$ for $n = 2, 3, 4, 5$, respectively. This is apparently approaching the limit $K(1, 2)$, as proposed.

Likewise, we can test whether, given 3 matrices in S_n, the 4 nontrivial linear combinations of these matrices are all in S_n with probability approaching $K(1, 2)^4 = 0.1113$ as the heuristic suggests. For example, $|S_3| = 294$ and of the 294^3 ordered triples, 2709504 or 10.66% satisfy this, which is close to the predicted 11.13%.

Finally, we consider some implications of the heuristic. Let $g(k)$ denote the order of $GL(k, 2)$, i.e., $g(k) = C(k, k, 2) = (2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})$. This counts the number of ordered bases of a k-dimensional vector space over $GF(2)$. If our heuristic holds true, then $N(n, 1, 2, n+1) \approx K(1, 2)^{2^{n+1}-1} 2^{(n+1)n^2}$ implies that the number of $(n+1)$-dimensional spaces of n by n matrices over $GF(2)$ of constant rank $n-1$ is $N(n, 1, 2, n+1)/g(n+1) \approx K(1, 2)^{2^{n+1}-1} 2^{(n+1)n^2}/g(n+1)$. Moreover, if conjugacy by $GL(n, 2)$ acts faithfully on the set of such spaces, then the number of orbits under conjugacy $\approx K(1, 2)^{2^{n+1}-1} 2^{(n+1)n^2}/(g(n)g(n+1))$. If it is not faithful, then the number will be slightly larger (but not by orders of magnitude - see the examples for $n = 3$ in Section 2 where the stabilizers all have order ≤ 6).

For $n = 1, \ldots, 10$, this gives (to 4 significant figures) respectively $0.1285, 0.08713, 5.388, 244200, 6.783 \times 10^{12}, 1.162 \times 10^{21}, 1.868 \times 10^{24}, 1.006 \times 10^{9}, 3.562 \times 10^{-54}, 4.986 \times 10^{-223}$. It is easy to see that our estimate on the number of orbits is tending to zero very fast. The above data suggests the following:

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 1-5, January 2010

ELA
http://math.technion.ac.il/iic/ela

CONJECTURE 3.1. *There exists an* $(n+1)$*-dimensional space of* n *by* n *matrices over* $GF(2)$ *of constant rank* $n-1$ *if and only if* $3 \leq n \leq 8$*.*

Our results in Section 2 prove this for $n \leq 5$. Note also that for $n = 3$ the heuristic predicts about 5.388 orbits or equivalently about 905 spaces of dimension 4 and constant rank 2, whereas there are actually 1176 of them.

Acknowledgment. The author thanks Rod Gow for introducing him to these problems and for useful feedback on this work.

REFERENCES

[1] L.B. Beasley. Spaces of rank-2 matrices over $GF(2)$. *Electron. J. Linear Algebra*, 5:11–18, 1999.
[2] L.B. Beasley and T.J. Laffey. Linear operators on matrices: the invariance of rank-k matrices. *Linear Algebra Appl.*, 133:175–184, 1990.
[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997.
[4] P.G. Buckheister. The number of n by n matrices of rank r and trace α over a finite field. *Duke Math. J.*, 39:695–699, 1972.
[5] K.Y. Lam and P. Yiu. Linear spaces of real matrices of constant rank. *Linear Algebra Appl.*, 195:69–79, 1993.
[6] G. Landsberg. Ber eine Anzahlbeslimmung und eine damit zusammenhangende Reihe, 1. *J. Reine Angew. Math.*, 111:87–88, 1893.
[7] D.B. Shapiro. *Compositions of quadratic forms.* De Gruyter Exp. Math., 33, 2000.