

Note

Unimodular Matrices and Parsons Numbers¹

AIDEN BRUEN*

Department of Mathematics, University of Western Ontario, London, Ontario, Canada N6A 3K7

DAVID WEHLAU†

*Department of Mathematics and Computer Science, Royal Military College of Canada,
Kingston, Ontario, Canada K7K 5L0; and Department of Mathematics and Statistics,
Queens University, Kingston, Ontario, Canada K7L 3N6*

AND

ZHANG ZHAOJI‡

Department of Mathematics, Zhejiang University, Hangzhou 310027, People's Republic of China

Communicated by the Managing Editors

Received November 23, 1993

Let $\{A_1, \dots, A_m\}$ be a set of m matrices of size $n \times n$ over the field \mathbb{F} such that $A_i \in SL(n, \mathbb{F})$ for $1 \leq i \leq m$ and such that $A_i - A_j \in SL(n, \mathbb{F})$ for $1 \leq i < j \leq m$. The largest integer m for which such a set exists is called the *Parsons number* for n and \mathbb{F} , denoted $m(n, \mathbb{F})$. We will call such a set of $m(n, \mathbb{F})$ matrices a *Parsons set*: such a set arises in a combinatorial setting (see [Z]). Parsons asserted (see [Z]) that $m(n, \mathbb{F}_q) \leq q^n$ if \mathbb{F}_q is the Galois field of order q . Here we will consider the case $n = 2$. Our result is the following.

THEOREM. *Let \mathbb{F} be any field. Let p be the characteristic of \mathbb{F} (possibly zero). Then $2 \leq m(2, \mathbb{F}) \leq 5$. Moreover, $m(2, \mathbb{F}) = 5$ if and only if $p = 5$ and \mathbb{F} contains a primitive cube root of unity. If $p = 3$ then $3 \leq m(2, \mathbb{F}) \leq 4$, and $m(2, \mathbb{F}) = 4$ if and only if \mathbb{F} contains a square root of -1 . Finally if $p \neq 2, 3$ and \mathbb{F} contains a square root of -3 , then $m(2, \mathbb{F}) = 4$ or $m(2, \mathbb{F}) = 3$ according as \mathbb{F} does or does not contain a square root of 33.*

* E-mail address: bruen@uwo.ca.

† E-mail address: wehlau@mast.queensu.ca.

‡ Supported by the Natural Science Foundations of Zhejiang Providence, P.R. China.

¹ This research is partially supported by NSERC grants.

We begin by observing that that $m(2, \mathbb{F}) \geq 2$ for every field \mathbb{F} . For example we may take

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}.$$

We remark without proof that $m(2, \mathbb{F}) = 2$ if and only $-3x^2 - 8$ is not a square in \mathbb{F} for all $x \in \mathbb{F}$. For example, $m(2, \mathbb{R}) = 2$.

For our upper bounds we begin by observing that $\{A_1^{-1}A_1 = I_2, A_1^{-1}A_2, \dots, A_1^{-1}A_m\}$ is also a Parsons set and thus we may assume that $A_1 = I_2$. In [Z], Zaks pointed out that $\det(A) = \det(A - I_2) = 1$ if and only if $\text{trace}(A) = 1$. Hence we know $\text{trace}(A_i) = 1$ for all $i \geq 2$. Thus for $i \geq 2$ the eigenvalues of A_i , ξ and $\bar{\xi}$, are the roots of $x^2 - x + 1$. We will repeatedly use the two facts $\xi\bar{\xi} = 1$ and $\xi + \bar{\xi} = 1$. Let $\tilde{\mathbb{F}}$ be the field $\mathbb{F}(\xi)$. Since the discriminant of $x^2 - x + 1$ is -3 , we see that $\tilde{\mathbb{F}} = \mathbb{F}$ if and only -3 is a square in \mathbb{F} . Now there exists $P \in GL(2, \tilde{\mathbb{F}})$ such that PA_2P^{-1} is in Jordan normal form, i.e., is of the form

$$\begin{pmatrix} \xi & 0 \\ \delta & \bar{\xi} \end{pmatrix}$$

with δ either 0 or 1 and with $\delta = 0$ if the eigenvalues ξ and $\bar{\xi}$ are different. Since $\{PI_2P^{-1} = I_2, PA_2P^{-1}, PA_3P^{-1}, \dots, PA_mP^{-1}\}$ is again a Parsons set, (as noted in [Z]) we may suppose, working in $\tilde{\mathbb{F}}$, that A_2 is in Jordan normal form. Note that $m(\mathbb{F}, n) \leq m(\tilde{\mathbb{F}}, n)$.

If $\xi = \bar{\xi}$ then $1 = \xi + \bar{\xi} = 2\xi$ (thus $p \neq 2$) and hence $\xi = 1/2$. Then $0 = (1/2)^2 - (1/2) + 1 = 3/4$. Hence $\xi = \bar{\xi}$ if and only if $p = 3$. Therefore we may write

$$A_2 = \begin{pmatrix} \xi & 0 \\ \delta & \bar{\xi} \end{pmatrix}$$

where $\delta = 0$ if $p \neq 3$, and $\delta \in \{0, 1\}$ if $p = 3$. Let us also write

$$A_i = \begin{pmatrix} a_i & b_i \\ c_i & 1 - a_i \end{pmatrix}$$

for $i \geq 3$.

Suppose $b_i = 0$ for some $i \geq 3$. Then $\{a_i, 1 - a_i\} = \{\xi, \bar{\xi}\}$. Since $\text{rank}(A_i - A_2) = 2$, we must have $a_i = \bar{\xi}$. Then $1 = \det(A_i - A_2) = -(\xi - \bar{\xi})^2 = 3$. Hence if $b_i = 0$ for some $i \geq 3$ then $p = 2$.

Assume there exists an $i \geq 3$ for which $b_i \neq 0$ (this will always be the case for $p \neq 2$). Then $\det(A_i) = 1$ implies $c_i = (-a_i^2 + a_i - 1)/b_i$. We solve

$\det(A_i - A_2) = 1$ for a_i . When $p \neq 3$, $\delta = 0$ and $a_i = (\xi - 1)/(2\xi - 1)$ and thus $c_i = -2/(3b_i)$ for $i \geq 3$. If on the other hand $p = 3$ then $\xi = \bar{\xi} = 2$ and we find $\delta = 1$ and $b_i = 1$.

Now suppose $p \neq 2, 3$. Then $a_i = (\xi - 1)/(2\xi - 1)$, $b_i \neq 0$ and $c_i = -2/(3b_i)$ whenever $i \geq 3$. Hence A_i is determined by b_i for all $i \geq 3$. From $1 = \det(A_i - A_j)$ for $3 \leq i < j$, we find that $f(b_i, b_j) = 0$ where $f(y, y) = x^2 - 7/2 xy + y^2$. Since $g(x) := f(x, b_3) = x^2 - 7/2 b_3 x + b_3^2$ has b_4 as a root and the discriminant of g is $(-7/2)^2 - 4 = 33/4$, we find that $b_4 \in \mathbb{F}$ if and only if 33 is a square in \mathbb{F} . In particular, if $p \neq 2, 3$ and if 33 is not a square in \mathbb{F} then $m(2, \mathbb{F}) \leq 3$. In fact, in these cases we have equality since the set

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \xi & 0 \\ 0 & \bar{\xi} \end{pmatrix}, \begin{pmatrix} \frac{\xi - 1}{2\xi - 1} & 1 \\ -\frac{2}{3} & \frac{\xi}{2\xi - 1} \end{pmatrix} \right\}$$

is a Parsons set.

Now from $1 = \det(A_i - A_3)$ we find that b_i is a root of the quadratic $g(x)$ for $i \geq 4$ and thus $m \leq 3 + 2 = 5$. Suppose now that $m = 5$. Since b_4 and b_5 are the roots of $g(x)$, we have $b_4 b_5 = b_3^2$ and $b_4 + b_5 = 7b_3/2$. Similarly $b_3 b_5 = b_4^2$ and thus $b_5 = b_3^2/b_4 = b_4^2/b_3$. Therefore, $b_3^3 = b_4^3 = b_5^3$ and thus $b_4 = \omega b_3$ and $b_5 = \omega^2 b_3$ where ω is a primitive cube root of unity. Also $7b_3/2 = b_4 + b_5 = (\omega + \omega^2) b_3 = b_3$ and thus $7 = 2$ and $p = 5$. We note that if $p = 5$ then $m(2, \mathbb{F}) \geq 4$ as the following set shows:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ -1 & 3 \end{pmatrix} \right\}.$$

Therefore, if $m(2, \mathbb{F}) = 5$ then $p = 5$ and \mathbb{F} contains a primitive cube root of unity. Conversely, if $p = 5$ and if \mathbb{F} contains ω , a primitive cube root of unity then taking $b_3 = 1$, $b_4 = \omega$, and $b_5 = \omega^2$ we get a Parsons set containing 5 matrices

Now we examine the two remaining case, namely $p = 2$ and $p = 3$.

Let $p = 2$. If $b_i \neq 0$ for some $i \geq 3$ then as above we find $c_i = -2/(3b_i) = 0$. Accordingly, $b_i c_i = 0$ for all $i \geq 3$. From this we find that

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \xi & 0 \\ 0 & \bar{\xi} \end{pmatrix}, \begin{pmatrix} \bar{\xi} & 0 \\ 1 & \xi \end{pmatrix}, \begin{pmatrix} \bar{\xi} & 1 \\ 0 & \xi \end{pmatrix} \right\}$$

is a Parsons set in \mathbb{F} if $p=2$ as is easily checked. It is also easy to check that the set of 3 matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

is a Parsons set in $\mathbb{Z}/2\mathbb{Z}$.

Let $p=3$ then we have seen that $b_i=1$ and thus

$$A_i = \begin{pmatrix} a_i & 1 \\ -a_i^2 + a_i - 1 & 1 - a_i \end{pmatrix}$$

for $i \geq 3$. Then $1 = \det(A_i - A_j) = -(a_i - a_j)^2$ for $3 \leq i < j$. Thus if $p=3$ and $m(2, \mathbb{F}) \geq 4$ then \mathbb{F} contains a square root of -1 . Also $m(2, \mathbb{F}) \leq 4$ since otherwise $a_4 - a_3$, $a_5 - a_3$ and $a_5 - a_4$ would form a set of 3 distinct square roots of -1 . Finally

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \right\}$$

is a Parsons set in $\mathbb{Z}/3\mathbb{Z}$.

REFERENCE

[Z] J. ZAKS, Parsons graphs of matrices, *Discrete Math.* **78** (1989), 187–193.