What does the first row of an invertible matrix look like?

Dave Witte Morris
University of Lethbridge, Alberta, Canada
http://people.uleth.ca/~dave.morris
Dave.Morris@uleth.ca

Abstract. Write down any three numbers as the first row of a 3×3 matrix. Unless all three of these numbers are zero, it is easy to fill out the other two rows to make a matrix that has an inverse. The problem is more interesting if we put restrictions on the numbers that are allowed (such as only allowing whole numbers) or allow matrix entries that are not numbers (such as using a polynomial $f(x,y,z)$ for a matrix entry). This leads to surprising connections with other areas of mathematics.

$$\begin{bmatrix} 9 & 0 & 5 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix}$$ Can we fill in the rest to make it invertible? $$\begin{bmatrix} 0 & 0 & 0 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix}$$

Eg. $$\begin{bmatrix} 0 & 0 & 0 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \begin{bmatrix} b_1 & * & * \\ b_2 & * & * \\ b_3 & * & * \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

top-left corner: $1 = 0\,b_1 + 0\,b_2 + 0\,b_3 = 0$. Nonsense!

Proposition

1st row of inv'ble matrix can be anything but all 0's.

Proof. $$\begin{bmatrix} a_1 & a_2 & a_3 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \quad \begin{matrix} a_1 \neq 0 \\ \Longrightarrow \end{matrix} \quad \begin{bmatrix} a_1 & a_2 & a_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ inv'ble.}$$

Question

What does the first row of an inv'ble matrix look like?

Answer: It can be anything but all 0's.

More interesting: **restrict the matrix entries.**

Requirement

Entries of matrices (including A^{-1}) must be integers.

Eg. $$\begin{bmatrix} 2 & 4 & 6 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \begin{bmatrix} b_1 & ? & ? \\ b_2 & ? & ? \\ b_3 & ? & ? \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

top-left corner: $1 = 2b_1 + 4b_2 + 6b_3 = 2(b_1 + 2b_2 + 3b_3)$
$\Longrightarrow$ odd = even. Nonsense!

Proposition

$[a_1\ a_2\ a_3]$ is 1st row of an inv'ble mat (integer entries)
$\iff$ *a_1, a_2, a_3 have no common factor.*

Key fact. Column operations preserve invertibility.
Add/subtract mults of one column from other cols.

$$\begin{bmatrix} 36 & 45 & 10 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \to \begin{bmatrix} 6 & 5 & 10 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \to \begin{bmatrix} 1 & 5 & 0 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix}$$

$$\begin{bmatrix} 36 & 45 & 10 \\ 7 & 9 & 2 \\ 3 & 4 & 1 \end{bmatrix} \leftarrow \begin{bmatrix} 6 & 5 & 10 \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \leftarrow \begin{bmatrix} 1 & 5 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \leftarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

What does 1st row of an inv'ble matrix look like?
All entries must be polynomials in x, y, z.

Eg. $$\begin{bmatrix} (x+2yz)^2 & x^2+2xyz+1 \\ x^2+2xyz-1 & x^2 \end{bmatrix}^{-1} = \begin{bmatrix} x^2 & -1-x^2-2xyz \\ 1-x^2-2xyz & (x+2yz)^2 \end{bmatrix}$$

Eg. $$\begin{bmatrix} x & y & z \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \begin{bmatrix} p(x,y,z) & ? & ? \\ q(x,y,z) & ? & ? \\ r(x,y,z) & ? & ? \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

top-left corner:
$1 = x\,p(x,y,z) + y\,q(x,y,z) + z\,r(x,y,z)$
$\Longrightarrow 1 = 0 \cdot p(0,0,0) + 0 \cdot q(0,0,0) + 0 \cdot r(0,0,0) = 0.$
Nonsense!

Proposition

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \begin{bmatrix} p_1 & ? & ? \\ p_2 & ? & ? \\ p_3 & ? & ? \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$\Longrightarrow a_1 p_1 + a_2 p_2 + a_3 p_3 = 1$
$\Longrightarrow (a_1, a_2, a_3)$ *is "unimodular"*

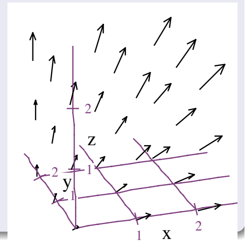
Serre (1955): We don't know whether every unimodular row (of polynomials) can be completed to an invertible matrix.

Fact

matrix is inv'ble $\iff$ rows are linearly independent.

Ques: Can every unimodular row (of polynomials) be completed to an invertible matrix?

We can look at this problem **geometrically**:
$(a_1, a_2, a_3) = (\, a_1(x,y,z),\, a_2(x,y,z),\, a_3(x,y,z)\,)$
defines a **vector field**.



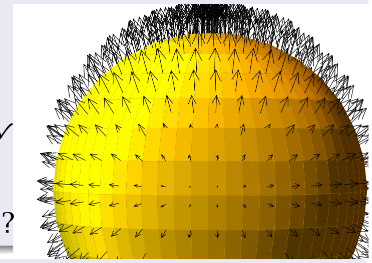
$$\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix} \text{ invertible}$$

$\Rightarrow$ (a_1, a_2, a_3) and (b_1, b_2, b_3) are lin indep *everywhere*.

Question: Given a unimodular vector field $\vec{A}$, is there a vf $\vec{B}$ that's lin indep from $\vec{A}$ everywhere?

Question: Given a unimodular vector field $\vec{A}$, is there a vf $\vec{B}$ that's lin indep from $\vec{A}$ everywhere?

Spse we only consider points on the unit sphere
$x^2 + y^2 + z^2 = 1$.
Let $\vec{A} = (x, y, z) =$ "up".
unimodular?
$x\,\boxed{x} + y\,\boxed{y} + z\,\boxed{z} = 1$ ✓
¿ Is there a vector field $\vec{B}$ that is never parallel to $\vec{A}$?



Topology theorem says **no**: every continuous vector fld on the sphere points straight up (or down) somewhere.
("You can't comb the hair on a coconut")

Question: Given a (unimodular) vector field $\vec{A}$, is there a vf $\vec{B}$ that's always lin indep from $\vec{A}$?

No on sphere. But what about $\mathbb{R}^3$?

Topologist's answer:

- $\vec{A}^{\perp}$ is a vector bundle on $\mathbb{R}^3$,
- $\mathbb{R}^3$ is contractible,
- so every vector bundle on $\mathbb{R}^3$ is trivial,
- every (nonzero) trivial vector bundle has a nowhere zero section.

$\therefore$ Yes, there is a continuous vector field $\vec{B}$.

But we want a *polynomial* vector field!

Question: Given a (unimodular) vector field $\vec{A}$, is there a vf $\vec{B}$ that is lin indep from $\vec{A}$ everywhere?

($\vec{A}$ and $\vec{B}$ are polynomials)

Answer (Quillen & Suslin 1976): **yes**.

Ques: *What does 1st row of inv'ble mat look like?*

Answer (for real numbers, integers, polynomials):
It must be unimodular.

Theorem (Quillen & Suslin 1976)
Every unimodular row of polynomials can be completed to an invertible matrix.

Exercise
Every unimodular row of integers can be completed to an invertible matrix.

Proof. $[a_1, a_2, a_3]$ unimodular row of integers
$\Rightarrow$ can reduce to $[1, 0, 0]$ by column ops.

Open problem *(Algebraic K-Theory)*
$[a_1, a_2, a_3]$ unimodular row of polynomials
$\overset{?}{\Rightarrow}$ can reduce to $[1, 0, 0]$ by column ops.

$[a_1, a_2, a_3]$ unimodular row of integers
$\rightsquigarrow [1, 0, 0]$ by column ops.

Theorem (Carter-Keller 1983)
$[a_1, a_2, a_3]$ unimodular row of integers
$\rightsquigarrow [1, 0, 0]$ by 50 column ops (over $\mathbb{Z}$).

Fact
$[a_1, a_2]$ unimodular row of integers
$\not\rightsquigarrow [1, 0]$ by bdd # of column ops (over $\mathbb{Z}$).

Theorem (Vsemirnov 2014)
$[a_1, a_2]$ unimodular row of integers
$\rightsquigarrow [1, 0]$ by 4 column ops (over $\mathbb{Z}[1/p]$).

Theorem. $[a_1, a_2]$ *unimodular row of integers*
$\rightsquigarrow [1, 0]$ *by 4 column ops (over* $\mathbb{Z}[1/p]$*).*

Easy proof

Assume Artin's Conjecture: $\forall r \neq \pm 1$, perfect square,
$\exists \infty$ primes q, s.t. r is primitive root modulo q:
$\{r, r^2, r^3, \ldots\} \bmod q = \{1, 2, 3, \ldots, q-1\}$
Assume $\exists q$ in any arithmetic progression $\{a + kb\}$.

$\forall [a, b]$, $\exists\, q = a + kb$, $\underline{\ p\ }$ is a primitive root mod q.

Proof.

$[a, b]$ $\quad q = a + kb$ prime, p is prim root
$\rightsquigarrow [q, b]$ $\quad p^\ell \equiv b \pmod{q}$; $p^\ell = b + k'q$
$\rightsquigarrow [q, p^\ell]$ $\quad p^\ell$ unit: can add *anything* to q
$\rightsquigarrow [1, p^\ell]$ $\quad \rightsquigarrow [1, 0]$ □

- W. H. Gustafson, P. R. Halmos, and J. M. Zelmanowitz: The Serre Conjecture. *Amer. Math. Monthly* 85 (1978) 357–359. http://www.jstor.org/stable/2321341
- T. Y. Lam: *Serre's Problem on Projective Modules.* Springer, New York, 2006.
- M. Vsemirnov: Short unitriangular factorizations of $SL_2(\mathbb{Z}[1/p])$. Quarterly. J. Math. 65 (2014) 279–290. MR 3179662, http://dx.doi.org/10.1093/qmath/has044

- A. V. Morgan, A. S. Rapinchuk, and B. Sury: Bounded generation of SL_2 over rings of S-integers with infinitely many units. https://arxiv.org/abs/1708.09262