proportions of invertible matrices

Canonical name	ProportionsOfInvertibleMatrices
Date of creation	2013-03-22 15:57:35
Last modified on	2013-03-22 15:57:35
Owner	Algeboy (12884)
Last modified by	Algeboy (12884)
Numerical id	16
Author	Algeboy (12884)
Entry type	Theorem
Classification	msc 15A33
Synonym	proportions invertible linear transformations

Let $GL(d,R)$ denote the invertible $d \times d$-matrices over a ring R, and $M_d(R)$ the set of all $d \times d$-matrices over R. When R is a finite field of order q, commonly denoted $GF(q)$ or $\mathbb{F}_q$, we prefer to write simply q. In particular, q is a power of a prime.

Proposition 1.

$$\frac{|GL(d,q)|}{|M_d(q)|} = \prod_{i=1}^{d} \left(1 - \frac{1}{q^i}\right).$$

Proof. The number of $d \times d$-matrices over a $GF(q)$ is q^{d^2}. When a matrix is invertible, its rows form a basis of the vector space $GF(q)^d$ and this leads to the following formula

$$|GL(d,q)| = q^{\binom{d}{2}} \prod_{i=1}^{d} (q^i - 1).$$

(Refer to `http://planetmath.org/OrdersAndStructureOfClassicalGroups`order of the general linear group.)

Now we prove the ratio holds:

$$\prod_{i=1}^{d} \left(1 - \frac{1}{q^i}\right) = \prod_{i=1}^{d} \frac{q^i - 1}{q^i} = \frac{1}{q^{\binom{d+1}{2}}} \prod_{i=1}^{d} (q^i - 1) = \frac{1}{q^{d^2}} q^{\binom{d}{2}} \prod_{i=1}^{d} (q^i - 1) = \frac{|GL(d,q)|}{|M_d(q)|}.$$

$\square$

Corollary 2. *As $q \to \infty$ with d fixed, the proportion of invertible matrices to all matrices converges to 1. That is:*

$$\lim_{q \to \infty} \frac{|GL(d,q)|}{|M_d(q)|} = 1.$$

Corollary 3. *As $d \to \infty$ and q is fixed, the proportion of invertible matrices decreases monotonically and converges towards a positive limit. Furthermore,*

$$\frac{1}{4} \leq 1 - \frac{q^2 - q + 1}{q^2(q-1)} \leq \prod_{i=1}^{d} \left(1 - \frac{1}{q^i}\right) \leq 1 - \frac{1}{q}.$$

Proof. By direct expansion we find

$$\prod_{i=1}^{\infty}(1-a_i) = 1 - \sum_{1\le i} a_i + \sum_{1\le i<j} a_i a_j - \sum_{1\le i<j<k} a_i a_j a_k + \cdots .$$

So setting $a_0 = 1$ and

$$a_{i+1} = a_i \sum_{j=i+1}^{\infty} \frac{1}{q^j} = a_i \frac{1}{q^i(q-1)}$$

for all $i \in \mathbb{N}$, we have

$$\prod_{i=1}^{\infty}\left(1-\frac{1}{q^i}\right) = \sum_{i=0}^{\infty}(-1)^i a_i.$$

As $a_i \ge 0$, $a_i \ge a_{i+1}$ for all $i \in \mathbb{N}$ and $a_i \to 0$ as $i \to \infty$, we may use Leibniz's theorem to conclude the alternating series converges. Furthermore, we may estimate the error to the N-th term with error within $\pm a_{N+1}$. Using $N = 2$ we have an estimate of $1-1/q$ with error $\pm\frac{1}{q^2(q-1)}$. Since $q \ge 2$ this gives $1/2$ with error $\pm 1/4$. Thus we have at least $1/4$ chance of choosing an invertible matrix at random. □

Remark 4. *$q = 2$ is the only field size where the proportion of invertible matrices to all matrices is less than $1/2$.*

Acknowledgements: due to discussions with Wei Zhou, silverfish and mathcam.