Curvarum Proprietatibus (Cambridge 1762). The translation into Russian of mathematical treatises by Al-Farabi and their publication in Kazakhstan at Alma Ata in 1972 serve to emphasize that the study of the history of mathematics knows no frontier.

A few details in conclusion, chosen not quite at random from selective explorations, will show that the intellectual profit from the use of the Library can be great. Here is C. Huygens studying the ancient problem of the quadrature of the circle (see *Oeuvres Complètes*, Volume 20, The Hague 1940). Here is evidence that Newton supposed the Creator to have made parts of absolute space impenetrable (see his *Opuscula*, Volume I, ed. J. Castillioneus, p.xxxiii, Lausanne and Geneva 1734). Here is Salmon handsomely giving credit to Boole for his part in originating the principles of linear transformation in modern algebra (George Salmon, *Lessons introductory to the Modern Higher Algebra*, third edition, Dublin 1876, p.103). Here is a copy of the third edition of Newton's *Principia* that once graced a library in Ballinlough. And here are collected works of W. Rowan Hamilton, J.J. Larmour, F. Severi and others.

Mathematical practitioners who wish to study in the Library are invited to ask the staff about rules and registration. The Academy believes that the mathematical aspects of its Library deserve to be better known; accordingly an increase in the number of mathematically interested readers would be a welcome development.

G.L.Huxley, M.R.I.A.
Honorary Librarian.

Note. I thank Professors J. T. Lewis and Anthony O' Farrell, both Members of the Academy, for helpful conversation and advice before the writing of this paper.

PROBABILITY IN FINITE SEMIGROUPS

Desmond MacHale

Let S be a finite non-empty set and let $*$ be a closed binary operation on S. For $x \in S$ let $C(x) = C_S(x)$, the centralizer of x in S, be $\{y \in S | x * y = y * x\}$, the set of all elements of S which commute with x. We define $Pr.(S)$ to be $\sum_{x \in S} |C(x)|/|S|^2$ so that $Pr.(S)$ is the probability that a pair of elements of S, chosen at random, will commute with each other.

Clearly, for $x, y \in S$, $x \in C(x)$, and $x \in C(y)$ if and only if $y \in C(x)$, but apart from these trivial restrictions there are no other restrictions on the values $Pr.(S)$ may have. Thus $1 \geq Pr.(S) \geq 1/|S|$ and the size of $Pr.(S)$ is a good indication of "how commutative" $\{S, *\}$ is, since $Pr.(S) = 1$ if and only if S is commutative.

If $\{G, *\}$ is a group then there are severe restriction on the values that $Pr.(G)$ may assume. For example we have the following (see [1] and [2])

(i) If $Pr.(G) > \frac{5}{8}$ then $Pr.(G) = 1$.
(ii) If $Pr.(G) > \frac{1}{2}$ then $Pr.(G) = \frac{1}{2} + \frac{1}{2^{2k+1}}$ for some k.
(iii) It is not possible to have $\frac{7}{16} < Pr.(G) < \frac{1}{2}$.

The bound given in (i) is the best possible and is attained for example by D_4, the group of all symmetries of the square.

At the lower end of the scale it is possible to make $Pr.(G)$ as small as we please in absolute terms, though not as small as $1/|G|$ unless G is trivial.

An easy calculation shows that $Pr.(S_3) = \frac{1}{2}$, where S_3 is the group of all permutations on three objects, and it is not difficult to show that $Pr.(A \times B) = Pr.(A).Pr(B)$ for the direct product of groups A and B. Consider then $G = S_3 \times S_3 \times S_3 \times \cdots \times S_3$, the direct product of n copies of S_3. $Pr.(G) = \frac{1}{2^n}$, which tends to zero as n gets large.

If $\{R, *\}$ is the multiplicative semigroup of a ring $\{R, +, *\}$, then again there are severe restrictions on the values $Pr.(R)$ can assume (see [2]).

Among these restriction we mention the following:

(i) $Pr.(R) \leq \frac{5}{8}$ for a non-commutative ring R.

This bound is attained by the following two rings of matrices over $\mathbf{Z}_2$

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

and

$$\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \quad \text{for all } a, b, c \in \mathbf{Z}_2 \right\}.$$

Note that the second of these rings is a ring with unity.

(ii) If p is the least prime dividing $|R|$ then

$$Pr.(R) \leq \frac{1}{p^3}(p^2 + p - 1),$$

with equality if and only if $(R : Z(R)) = p^2$, where $Z(R)$ is the centre of R.

In this note we concentrate on the case where $\{S, *\}$ is a semigroup and we show that a finite semigroup can be as commutative or as noncommutative as we like.

For each $n \geq 4$ we show that there is a semigroup T_n of order n with $Pr.(T_n) = (n^2 - 2)/n^2$, which is as large as possible. For $n \geq 4$ let $T_n = \{a_1, a_2, \ldots, a_n\}$ and define a binary operation $*$

on T_n by $a_n * a_{n-1} = a_2$, with all other products equal to a_1. For example, $\{T_4, *\}$ looks like this.

$*$	a_1	a_2	a_3	a_4
a_1	a_1	a_1	a_1	a_1
a_2	a_2	a_1	a_1	a_1
a_3	a_1	a_2	a_1	a_1
a_4	a_1	a_1	a_2	a_1

$\{T_n, *\}$ is closed and $(x * y) * z = a_1 = x * (y * z)$ for all $x, y, z \in T_n$, so $\{T_n, *\}$ is a semigroup. It is easy to see that $Pr.(T_n) = (n^2 - 2)/n^2$ and this fraction can be made as close as we like to 1 by taking n large enough.

At the lower end of the scale we show that for each n there exists a semigroup W_n with $Pr.(W_n) = \frac{1}{n}$, which is as small as possible.

Let $W_n = \{b_1, b_2, \ldots, b_n\}$ and define a binary operation $\bullet$ on W_n by $b_i \bullet b_j = b_j$, for all i, j. For example $\{W_3, \bullet\}$ is given by the following table.

$\bullet$	b_1	b_2	b_3
b_1	b_1	b_2	b_3
b_2	b_1	b_2	b_3
b_3	b_1	b_2	b_3

$\{W_n, \bullet\}$ is closed and for all $x, y, z \in W_n$

$$(x \bullet y) \bullet z = y \bullet z = z = x \bullet z = x \bullet (y \bullet z),$$

So $\{W_n, \bullet\}$ is a semigroup. Further $b_i \bullet b_j = b_j \bullet b_i \iff b_i = b_j$. So $Pr.(W_n) = \dfrac{1}{n}$.

Problems

1. Given a rational number $0 < \frac{m}{n} < 1$ does there exist a semigroup S with $Pr.(S) = \frac{m}{n}$? Note that $Pr.(S_1 \times S_2) = Pr.(S_1)Pr.(S_2)$ for the direct product of semigroups so that given some values of $\frac{m}{n}$ we can generate others.

2. Are there any restrictions on $Pr.(S)$ for other algebraic structures such as inverse semigroups, near-rings, bands or groupoids?

There are many other questions that can be asked about probability in finite algebraic systems. For example, we ask "what is the probability that an element of a semigroup S has an inverse?" We call this probability $I(S)$. If S does not have identity then $I(S) = 0$ so we assume S has identity e. We ask the following question: For each N, is it possible to choose semigroups of order n which satisfy $I(S) = \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots \frac{n}{n}$?

It is easy to show that for each n we can achieve the value $I(S) = \frac{1}{n}$, as follows. The case $n = 1$ is trivial, so suppose that $n \geq 2$. Consider a semigroup K of order $n-1$ such that k does not have identity (for example, put every product equal to a fixed element). Then adjoin to K an element e such that $e \bullet x = x \bullet e = x$ for all $x \in K$ and $e \bullet e = e$.

Then $I\big(K \cup \{e\}\big) = \frac{1}{n}$.

Also, we can achieve $\frac{n}{n} = 1$ because there is always a group of order n, namely the cyclic group $\{\mathbf{Z}_n, \oplus\}$. Thus for $n = 2$ we can achieve $\frac{0}{2}, \frac{1}{2}, \frac{2}{2}$. We show that for $n = 3, 4$ the other values are also achievable.

For $n = 3$, $\{\mathbf{Z}_3, \otimes\}$ gives $I(S) = \frac{2}{3}$.

(In fact, for p a prime $I\{\mathbf{Z}_p, \otimes\} = \frac{p-1}{p}$, since $\mathbf{Z}_p - \{0\}$ is a group under $\otimes$.)

For $n = 4$, $\{\mathbf{Z}_4, \oplus\}$ gives $I(S) = \frac{2}{4}$ while $\{GF(4), \otimes\}$ gives $\frac{3}{4}$.

In fact $\{GF(p^n), \otimes\}$ gives $\frac{p^n-1}{p^n}$ for any prime power p^n. In general $\{\mathbf{Z}_n, \otimes\}$ gives $\phi(n)/n$, where $\phi(n)$ is the Euler ϕ-function.

3. Find semigroups of order 5 for which the values $\frac{2}{5}$ and $\frac{3}{5}$ are achieved.

Note that $I(A \times B) = I(A)I(B)$ for the direct product of semigroups A and B and this fact can be of use in generating the *values* required in problem 3, though not necessarily among semigroups of order 5. Finally, we can consider $I(R)$ where R is a finite ring with unity. Let $[n]$ be the greatest integer function. We quote the following theorem found in [3].

Theorem. *If* $I(R) > \frac{1}{|R|^2}\big(|R| - [\sqrt{R}]\big)$, *the* $I(R) = \frac{1}{|R|}\big(|R| - 1\big)$ *and* R *is a finite field.*

$\mathbf{Z}_{p^2}$ for p a prime shows that this result is best possible.

References

[1]. W. H. Gustafson, *What is the probability that two group elements commute?* American Math. Monthly **80** (1973) 1031–1034.

[2]. D. MacHale, *Commutativity in finite rings*, American Math. Monthly **83** (1976) 30–32.

[3]. D. MacHale, *Wedderburn's Theorem revisited.* Bull. Irish Math. Soc **17** (1986) 44–46.

Desmond MacHale
Department of Mathematics
University College Cork