On cyclically shifted strings

K. Bärwinkel, H.-J. Schmidt [1], J. Schnack

Universität Osnabrück, Fachbereich Physik
Barbarastr. 7, 49069 Osnabrück, Germany

Abstract

If a string is cyclically shifted it will re–appear after a certain number of shifts, which will be called its *order*. We solve the problem of how many strings exist with a given order by applying the MOEBIUS inversion principle. This problem arises in the context of quantum mechanics of spin systems.

1 Introduction and definitions

Let $\mathcal{S}(A,N)$ denote the set of strings $a = \langle a_1, \ldots, a_N \rangle$ of natural numbers $a_n \in \{0, \ldots, A-1\}$. There are exactly A^N such strings. For any $a \in \mathcal{S}(A,N)$ let $\Sigma(a) \overset{\text{def}}{=} \sum_{n=0}^{N} a_n$ and $T(a) \overset{\text{def}}{=} \langle a_N, a_1, a_2, \ldots, a_{N-1} \rangle$. T is the cyclic shift operator. If T^n denotes the nth power of T, $n \in \mathbb{N}$, it follows that $T^N = T^0 = \mathbb{1}_{\mathcal{S}(A,N)}$. We consider two equivalence relations on $\mathcal{S}(A,N)$. For $a, b \in \mathcal{S}(A,N)$ we define

$$a \sim b \Leftrightarrow \Sigma(a) = \Sigma(b) \tag{1}$$

and

$$a \approx b \Leftrightarrow a = T^n(b) \text{ for some } n \in \mathbb{N}. \tag{2}$$

Obviously, $a \approx b$ implies $a \sim b$ since the sum of the numbers in a string is invariant under permutations.
The aim of this article is to analyze the structure of the equivalence classes of strings with respect to $\sim$ and $\approx$. The main question will be: How many $\approx$-equivalence classes of a given size exist? Or: How many $\approx$-equivalence classes of a given size exist which are contained in a certain $\sim$-equivalence class? This problem can, of course, be solved in a straight-forward manner for any given A and N, either by

[1] corresponding author: hschmidt@uos.de,
http://www.physik.uni-osnabrueck.de/makrosysteme/

Preprint submitted to COMBINATORICA 16 NOVEMBER 2000

hand or by means of a simple computer program. We are rather seeking explicit formulae which answer the above questions.
The problem arises in the context of quantum mechanics of spin rings with a cyclically symmetric coupling between the N individual spins. Any individual spin can assume A different states and the total system can assume A^N different states. More precisely: The total Hilbert space of the problem possesses an orthonormal basis of product states parametrized by the set $\mathcal{S}(A, N)$. According to the symmetries of the problem it is possible to split the total Hilbert space into a sum of orthogonal subspaces which are invariant under the Hamiltonian of the problem. These subspaces are closely connected to the equivalence classes of strings defined above. For more details see [1–3].

2 Strings with constant sum

For any $a \in \mathcal{S}(A, N)$ we denote the corresponding equivalence class $[a]_\sim$ of strings having the same sum by

$$\mathcal{S}(A, N, M) \quad \text{where } M \stackrel{\text{def}}{=} \Sigma(a). \tag{3}$$

Obviously, $\mathcal{S}(A, N)$ is a disjoint union

$$\mathcal{S}(A, N) = \bigcup_{M=0\ldots N(A-1)} \mathcal{S}(A, N, M) \tag{4}$$

and the total number of strings satisfies

$$|\mathcal{S}(A, N)| = A^N = \sum_{M=0\ldots N(A-1)} |\mathcal{S}(A, N, M)| \,. \tag{5}$$

The problem of determining the number of strings with a constant sum $|\mathcal{S}(A, N, M)|$ is equivalent to the problem of calculating the probability distribution of the sum of N independent, finite, uniformly distributed random variables. An example would be the probability of scoring the sum M in a throw with N dice with A faces. Geometrically, this is the problem of how many lattice points are met if you cut a hypercube containing A^N lattice points perpendicular to its main diagonal.
The solution to this problem is known since long and traces back to Abraham de MOIVRE [4]:

$$|\mathcal{S}(A, N, M)| = \sum_{n=0}^{\lfloor \frac{M}{A} \rfloor} (-1)^n \binom{N}{n} \binom{N-1+M-nA}{N-1}, \tag{6}$$

where $\lfloor x \rfloor$ denotes the largest integer $\leq x$. The proof is straight-forward using the generating function (see e. g. [5])

$$\left(\sum_{a=0}^{A-1} z^a \right)^N = \sum_{m=0}^{N(A-1)} |\mathcal{S}(A, N, m)| \, z^m. \tag{7}$$

3 Cycles of strings

We will call the equivalence classes $\mathbf{a} = [a]_\approx, \quad a \in \mathcal{S}(A, N)$ of strings which are connected by cyclic shifts "cycles". The different sets of cycles will be denoted by

$$\mathcal{C}(A, N) \stackrel{\text{def}}{=} \mathcal{S}(A, N)/\approx, \quad \mathcal{C}(A, N, M) \stackrel{\text{def}}{=} \mathcal{S}(A, N, M)/\approx . \tag{8}$$

This notation appears natural since cycles are the orbits of the cyclic group

$$G \stackrel{\text{def}}{=} \{T^n : n = 0, \ldots, N-1\} \cong \mathbb{Z}_N \tag{9}$$

operating on strings in the way defined above. Hence cycles can at most contain N strings. The number of strings contained in a cycle will be called its "order". "Proper cycles" are defined as those of maximal order N, "epicycles" are cycles of order less than N. Special epicycles are those containing exactly one constant string $a = \langle i, i, \ldots, i \rangle, i \in \{0, \ldots, A-1\}$. These will be of order one and are called "monocycles". Obviously, there are exactly A monocycles.
Generally, the orbit of a group G generated by the operation on some element a will be isomorphic to the quotient set G/G_a, where G_a is defined as the subgroup of all transformations leaving a fixed. In our case G_a will be isomorphic to $\mathbb{Z}_k$ where k is a divisor of N and $\mathbf{a}$ will be of order $n = \frac{N}{k}$. k will be called the "complementary order" of $\mathbf{a}$. The case $k = 1$ corresponds to proper cycles, whereas the case $k = N$ yields monocycles.
To put it differently: If a string $a \in \mathcal{S}(A, N)$ consists of k copies of a substring $b \in \mathcal{S}(A, n)$, $kn = N$, it will generate an epicycle $\mathbf{a} = [a]_\approx$ containing at most n strings. $\mathbf{a}$ contains exactly n strings iff b itself generates a proper cycle $\mathbf{b} \in \mathcal{C}(A, n)$. Conversely, any epicycle $\mathbf{a}$ of order n consists of strings which are k copies of substrings b belonging to proper cycles $\mathbf{b}$. Moreover, if $\mathbf{a} \in \mathcal{C}(A, N, M)$ is of order n the corresponding proper cycle $\mathbf{b}$ will satisfy $\mathbf{b} \in \mathcal{C}(A, n, m)$ with $M = km$. Thus we obtain the following

Lemma 1 *(1) The order n of any cycle $\mathbf{a} \in \mathcal{C}(A, N, M)$ is a divisor of N.*

(2) Moreover, in this case $m \stackrel{\text{def}}{=} \frac{Mn}{N}$ will be an integer.

Hence the order of cycles will always belong to the following set:

Definition 1 $\mathcal{D}(A, N, M) \stackrel{\text{def}}{=} \{n \in \mathbb{N} : n|N \text{ and } N|Mn\}$, and the complementary order $k = \frac{N}{n}$ will always belong to

Definition 2 *$\mathcal{C}D(N, M)$, defined as the set of common divisors of N and M.*

In passing we note that if N is a prime number, then there will be only proper cycles and exactly A monocycles, as mentioned above, hence N will divide $A^N - A$, which is essentially FERMAT's theorem of 1640, cf. [6], Theorem 2.13

Definition 3 *Let $\mathcal{N}(A, N, M, n)$ denote the number of cycles $\mathbf{a} \in \mathcal{C}(A, N, M)$ of order n and $\mathcal{M}(A, N, M, n)$ the number of strings belonging to these cycles:*

$$\mathcal{M}(A, N, M, n) \stackrel{\text{def}}{=} \mathcal{N}(A, N, M, n)n. \tag{10}$$

According to the preceding discussion the following holds:

Lemma 2

$$\mathcal{M}(A, N, M, n) = \begin{cases} \mathcal{M}(A, n, \frac{Mn}{N}, n) & : \quad \textit{if } n \in \mathcal{D}(A, N, M) \\ 0 & : \quad \textit{else} \end{cases}, \tag{11}$$

$$|\mathcal{S}(A, N, M)| = \sum_{n \in \mathcal{D}(A,N,M)} \mathcal{M}(A, N, M, n) \tag{12}$$

$$= \sum_{k \in \mathcal{C}D(N,M)} \mathcal{M}(A, \frac{N}{k}, \frac{M}{k}, \frac{N}{k}). \tag{13}$$

Together with (6) this yields a recursion relation for $\mathcal{M}(A, N, M, n)$. It is, however, possible to obtain an explicit formula by means of MOEBIUS' inversion principle, which will be shown in the next section.

4 Explicit formula for $\mathcal{M}(A, N, M, n)$

We recall the definition of the MOEBIUS function μ:

Definition 4

$$\mu(\nu) \stackrel{\text{def}}{=} \begin{cases} 1 & : \quad \textit{if } \nu = 1, \\ (-1)^m & : \quad \textit{if } \nu \textit{ is a product of } m \textit{ distinct primes,} \\ 0 & : \quad \textit{else.} \end{cases} \tag{14}$$

The MOEBIUS inversion principle may be formulated as follows:

Theorem 1 *Let $n \in \mathbb{N}$ and $\mathcal{D}(n)$ denote the set of divisors of n, further let f and g be two functions defined on $\mathcal{D}(n)$. Then*

$$g(\nu) = \sum_{d|\nu} f(d) \quad \textit{for all } \nu \in \mathcal{D}(n), \tag{15}$$

if and only if

$$f(\nu) = \sum_{d|\nu} \mu(d) g(\frac{\nu}{d}) \quad \textit{for all } \nu \in \mathcal{D}(n). \tag{16}$$

It can be easily checked that this formulation is equivalent to the usual one which refers to functions defined for all natural numbers, cf. for example [6], Theorem 6.14. From our formulation we may derive a slightly generalized principle:

Theorem 2 *Let $n_i \in \mathbb{N}$, i=1, ..., r, and $\mathcal{C}D(n_1, \ldots, n_r)$ denote the set of common divisors of $n_1, \ldots, n_r$, further let f and g be two functions defined on $\mathcal{D} \stackrel{\text{def}}{=} \left\{(\frac{n_1}{d}, \ldots, \frac{n_r}{d}) | d \in \mathcal{C}D(n_1, \ldots, n_r)\right\}$. Then*

$$g(\nu_1, \ldots, \nu_r) = \sum_{d \in \mathcal{C}D(\nu_1, \ldots, \nu_r)} f(\frac{\nu_1}{d}, \ldots, \frac{\nu_r}{d}) \quad \textit{for all } (\nu_1, \ldots, \nu_r) \in \mathcal{D}, \tag{17}$$

if and only if

$$f(\nu_1, \ldots, \nu_r) = \sum_{d \in \mathcal{C}D(\nu_1, \ldots, \nu_r)} \mu(d) g(\frac{\nu_1}{d}, \ldots, \frac{\nu_r}{d}) \quad \textit{for all } (\nu_1, \ldots, \nu_r) \in \mathcal{D}. \tag{18}$$

This theorem follows from Theorem 1 since the set $\mathcal{C}D(n_1, \ldots, n_r)$ is identical to the set $\mathcal{D}(n)$, if n denotes the greatest common divisor of $n_1, \ldots, n_r$ and the domains $\mathcal{D}(n)$ and $\mathcal{D}$ of the respective functions are in $1:1$ correspondence.

Theorem 2 may be applied in order to solve (13) for $\mathcal{M}(A, N, M, N)$ if we set $g(N, M) = |\mathcal{S}(A, N, M)|$ and $f(N, M) = \mathcal{M}(A, N, M, N)$.
Using (6), we eventually obtain the following

Theorem 3

$$\mathcal{M}(A, N, M, N) = \sum_{n \in \mathcal{D}(A,N,M)} \mu(\frac{N}{n}) \sum_{\nu=0}^{\lfloor \frac{Mn}{NA} \rfloor} (-1)^{\nu} \binom{n}{\nu} \binom{n - 1 + \frac{Mn}{N} - \nu A}{n - 1}, \tag{19}$$

Let $\mathcal{M}(A, n)$ denote the number of strings belonging to cycles of order n, irrespective of M. This number does not depend on the total length N of the strings. By an

Order n	Number of cycles of order n
1	5
2	10
3	40
4	150
6	2580
12	20343700

Table 1
Number of cycles of order n for $N = 12$ and $A = 5$.

analogous reasoning as above we may conclude

Theorem 4

$$\mathcal{M}(A, n) = \sum_{k|n} \mu(\frac{n}{k}) A^k. \tag{20}$$

From this expression the number of cycles is obtained by division by n. Note that $n|\mathcal{M}(A, n)$, hence (20) generalizes FERMAT's original result to the case where n need not be prime.
Finally we give a numerical example for $N = 12$ and $A = 5$ in table 1.

Acknowledgement

We would like to thank an anonymous referee to COMBINATORICA for having drawn our attention to the MOEBIUS inversion principle.

References

[1] D. Kouzoudis, *Heisenberg $s = \frac{1}{2}$ ring consisting of a prime number of atoms*, J. Magn. Magn. Mater. **173** (1997) 259

[2] D. Kouzoudis, *Exact analytical partition function and energy levels for a Heisenberg ring of $N = 6$ spin 1/2 sites*, J. Magn. Magn. Mater. **189** (1998) 366

[3] K. Bärwinkel, H.-J. Schmidt, J. Schnack, *Structure and relevant dimension of the Heisenberg model and applications to spin rings*, J. Magn. Magn. Mater. **212** (2000) 240-250

[4] A. de Moivre, *Miscellanea Analytica*, (1730), 191-197

[5] W. Feller, *An introduction to probability theory and its applications*, Vol. 1, 3. ed., John Wiley & Sons, New York (1968) chapter XI.7, problem 18

[6] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, New York (2000)