

# Universal cycles for combinatorial structures

Fan Chung

*Bell Communications Research, Morristown, NJ 07960, USA*

Persi Diaconis

*Harvard University, Cambridge, MA 02139, USA*

Ron Graham

*AT&T Bell Laboratories, Murray Hill, NJ 07974, USA*

Received 2 July 1990

Revised 12 April 1991

## *Abstract*

Chung, F., P. Diaconis and R. Graham, Universal cycles for combinatorial structures, *Discrete Mathematics* 110 (1992) 43–59

In this paper, we explore generalizations of de Bruijn cycles for a variety of families of combinatorial structures, including permutations, partitions and subsets of a finite set.

## **1. Introduction**

The cyclic sequence  $C$  of 16 0's and 1's shown in Fig. 0 has the following unlikely property. If we list each of the 16 possible blocks of 4 consecutive symbols of  $C$ , it turns out that they are all different. As a consequence, it follows that *every possible* 0–1 sequence of length 4 occurs this way (uniquely). The cycle  $C$  is an example of what has come to be known as a *de Bruijn cycle*. More generally, a (binary) de Bruijn cycle  $C_n$  of order  $n$  is defined to be a cyclic sequence  $(x_0, x_1, \dots, x_{2^n-1})$  where  $x_i = 0$  or 1, and each possible binary sequence of length  $n$  occurs uniquely as  $(x_{i+1}, \dots, x_{i+n})$  for some  $i$ , where index addition is performed modulo  $2^n$ . The study of such cycles has had a long and distinguished history, and has arisen in a variety of contexts, such as design of Sanskrit memory wheels, digital fault testing, pseudo-random number generation, modern public-key cryptographic schemes, and even for use by illusionists in various mind-reading effects, to mention a few. (For an overview of this history, and indeed, the whole topic of de Bruijn cycles, the reader can consult [1, 5, 21, 14].

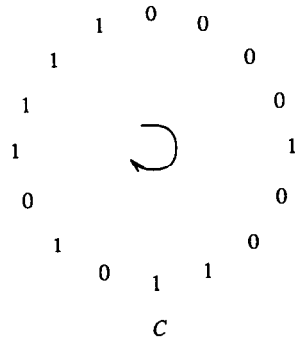


Fig. 0. A de Bruijn cycle of order 4.

Among the fundamental questions one might ask concerning de Bruijn cycles are:

- (i) Do de Bruijn cycles *always exist* for each  $n$ ?
- (ii) If so, *how many* are there?
- (iii) How does one *construct* them?
- (iv) In a given de Bruijn cycle  $C$ , is there an easy way of determining the  $i$ th block as a function of  $i$ ?
- (v) How can one ‘invert’ this process in  $C$ . That is, for each given block, *where* is it in  $C$ ?
- (vi) How can one ‘cut down’ a de Bruijn cycle  $C$ . That is, when is it possible to remove elements from  $C$  so that the resulting contracted cycle  $C'$  still has *distinct* blocks of length  $n$  (although some now will be missing). In the same spirit, how can one ‘build up’ or ‘combine’ de Bruijn cycles?
- (vii) What are the analogues for larger alphabets ( $k$  symbols rather than 2), or more dimensions (e.g., a de Bruijn ‘torus’ rather than a cycle), etc.

We will summarize some of the known answers to some of these questions in Section 3.

The thrust of this paper will be to consider the analogous situation for a variety of other combinatorial structures, rather than binary  $n$ -tuples. In particular, we will outline what is known for *permutations* of an  $n$ -set (Section 4), *partitions* of an  $n$ -set (Section 5), and  $k$ -sets of an  $n$ -set (Section 6). In Section 2, we formulate our problem in a general setting, and in Section 3, we interpret de Bruijn cycles in this formulation. Finally, in Section 7, we describe possible future directions.

## 2. A general formulation

We begin by being given some family  $\mathcal{F}_n$  of combinatorial objects of ‘rank  $n$ ’. We denote their number by  $m := |\mathcal{F}_n|$ . We assume that each  $F \in \mathcal{F}_n$  is ‘generated’ or specified by some sequence  $\langle x_1, \dots, x_n \rangle$ , where  $x_i \in A$ , for some fixed alphabet  $A$ .

We will say that  $U = (a_0, a_1, \dots, a_{m-1})$  is a *universal cycle* for  $\mathcal{F}_n$  (or *U-cycle*, for short) if  $\langle a_{i+1}, \dots, a_{i+n} \rangle$ ,  $0 \leq i < m$ , runs through each element of  $\mathcal{F}_n$  exactly once, where index addition is performed modulo  $n$ .

Now we can ask the standard questions: do *U-cycles* for  $\mathcal{F}_n$  exist, if so how many, how do you construct them, invert them, combine them, extend them, etc. Of course, it is clear that some *U-cycles* might be better than others for some of these purposes. When this is so, how do we find ‘good’ ones.

In addition to their inherent combinatorial interest, one might also ask how one might use these *U-cycles*.

### 3. de Bruijn cycles

We next sketch the standard approach used for treating de Bruijn cycles. In this case,

$$\mathcal{F}_n = B_n = \{0, 1\}^n = \{(x_1, \dots, x_n) \mid x_i \in \{0, 1\}, 1 \leq i \leq n\}, \quad m = 2^n$$

and each binary  $n$ -tuple  $(x_1, \dots, x_n)$  is just represented by itself, i.e.,

$$\langle x_1, \dots, x_n \rangle \leftrightarrow (x_1, \dots, x_n).$$

(This will not be the case in most of the later situations.)

The first step in constructing potential *U-cycles* for  $B_n$  is to construct the (directed) *transition graph*  $G_n$  for  $B_n$ . The *vertices* of  $G_n$  are all the  $n$ -tuples  $\{0, 1\}^n$ . There is a *directed edge* (= arc) from  $(x_1, \dots, x_n)$  to  $(y_1, \dots, y_n)$  provided  $x_2 = y_1, x_3 = y_2, \dots, x_n = y_{n-1}$ . Thus, arcs look like  $((x_1, \dots, x_n), (x_2, \dots, x_n, x_{n+1}))$ . What this indicates is that it is possible to go from  $(x_1, \dots, x_n)$  to  $(x_2, \dots, x_{n+1})$  in a potential *U-cycle*, namely, when the block  $\dots x_1, x_2, \dots, x_n, x_{n+1} \dots$  occurs.

We illustrate the graphs  $G_2$  and  $G_3$  in Fig. 1.

From this point of view, a *U-cycle* for  $B_n$  corresponds exactly to a directed circuit in  $G_n$  going through each vertex exactly once, i.e., a *Hamiltonian circuit* for  $G_n$ . This is both good news and bad news. The good news is that our problem has been reduced to finding a very familiar object in graph theory, namely, Hamiltonian circuits. The bad news is that these objects are well known to be difficult to find! In fact, it is an NP-complete problem to decide if a graph in general even has a Hamiltonian circuit.

Fortunately, we have a way around this problem in this case. What we can do is to define another digraph  $G_n^*$ , called the *arc digraph* of  $G_n$ , as follows. The *vertices* of  $G_n^*$  will just be the arcs of  $G_n$ . In particular the arc  $((x_1, \dots, x_{n-1}, x_n), (x_2, \dots, x_n, x_{n+1}))$  will correspond to the vertex labelled with the  $(n-1)$ -tuple  $(x_2, \dots, x_n)$  in  $G_n^*$ . The *arcs* of  $G_n^*$  will be all pairs of vertices  $((y_1, \dots, y_{n-1}), (y_2, \dots, y_n))$  in  $G_n^*$ , i.e., so that the ‘head’ of the first vertex label is equal to the ‘tail’ of the second vertex label. In Fig. 2, we show  $G_2^*$

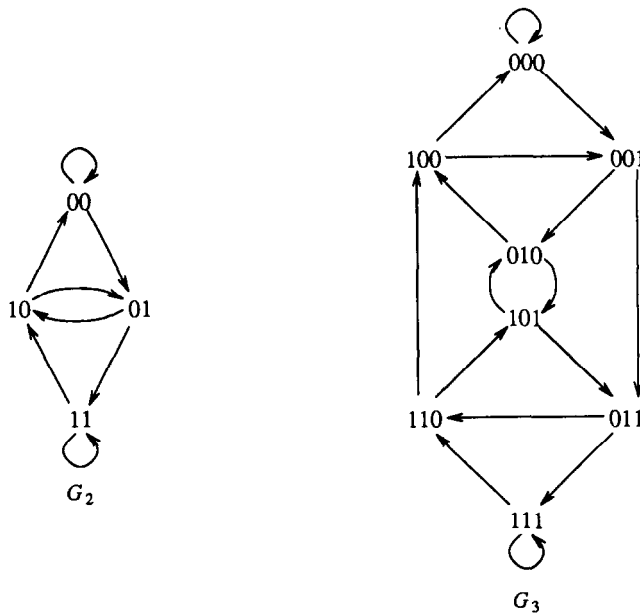


Fig. 1. The graphs  $G_2$  and  $G_3$ .

and  $G_3^*$ . It is clear now that a Hamiltonian circuit in  $G_n$  corresponds exactly to an ‘Eulerian’ circuit in  $G_n^*$ , i.e., a (directed) circuit passing through each arc exactly once. The advantage of this transformation is that Eulerian circuits in digraphs are easy to detect. To state this precisely, let us call a digraph  $G$  *balanced* if for every vertex  $v$  of  $G$ ,  $\text{indegree}(v) = \text{outdegree}(v)$ . Also, call  $G$  *strongly connected* if for any vertices  $u$  and  $v$  of  $G$ , there is a directed path in  $G$  from  $u$  to  $v$ .

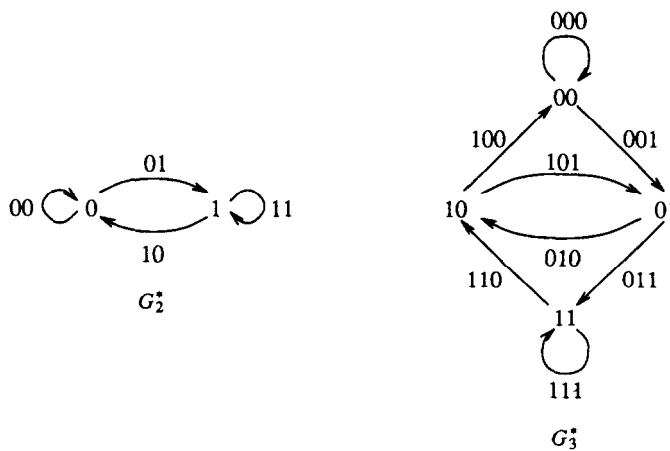


Fig. 2. The arc digraphs  $G_2^*$  and  $G_3^*$ .

**Fact.**  $G$  has an Eulerian circuit if and only if  $G$  is balanced and strongly connected.

It is not difficult to see that  $G_n^*$  is balanced and strongly connected, and so is Eulerian. This in turn shows that  $G_n$  is Hamiltonian, i.e., has a  $U$ -cycle. Notice that  $G_n^*$  is isomorphic to  $G_{n-1}$ . A more careful analysis shows that in fact  $G_n^*$  has exactly  $2^{2^n-n}$  different Eulerian cycles. For a good discussion of this topic as well as various generalizations such as  $k$ -symbol alphabets, the reader is referred to [14, 15, 18].

In the next three sections we will attempt to apply the same analysis (with decreasing success) to permutations, partitions and  $k$ -set of an  $n$ -set, respectively.

#### 4. Permutations

Let us denote by  $S_n$  the set of all  $n!$  permutations (or arrangements) of  $\{1, 2, \dots, n\}$ . If  $\bar{a} = (a_1, a_2, \dots, a_n)$  and  $\bar{b} = (b_1, b_2, \dots, b_n)$  each are  $n$ -tuples of distinct integers we will say that  $\bar{a}$  and  $\bar{b}$  are *order-isomorphic*, written  $\bar{a} \sim \bar{b}$ , if

$$a_i < a_j \Leftrightarrow b_i < b_j.$$

A  $U$ -cycle  $U_n = (a_0, a_1, \dots, a_{n!-1})$ ,  $a_i \in \{1, 2, \dots, N\}$ , for  $S_n$  will be  $n!$ -tuple such that each  $\sigma \in S_n$  is *order-isomorphic* to exactly one block  $(a_{i+1}, \dots, a_{i+n})$ , where, of course, index addition is performed modulo  $n!$ . It is clear why we must in general take  $N > n$  since blocks of length  $n$  must always consist of  $n$  distinct symbols. An example of  $U$ -cycle for  $S_3$  is

$$1\ 4\ 5\ 2\ 4\ 3.$$

To begin the process of constructing  $U$ -cycles of  $S_n$  we imitate the analysis used for de Bruijn cycles and construct the transition graph  $G_n$  for  $S_n$ . We illustrate this for  $N = 3$  in Fig. 3.

The arcs of  $G_n$  are defined as follows. Suppose (for  $n = 3$ ) we have the sequence  $\dots 4\ 5\ 2\ x \dots$  where we are suppressing commas. Now  $452 \sim 231$ . The next 3-block  $52x$  could have three possibilities. If  $x = 1$  then  $521 \sim 321$  so that we get the arc  $231 \rightarrow 321$ . If  $x = 3$  then  $523 \sim 312$  and we have the arc  $231 \rightarrow 312$ .

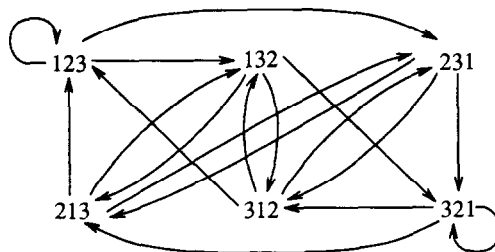


Fig. 3.  $G_3$ .

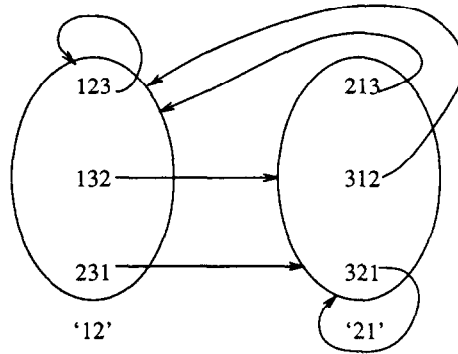
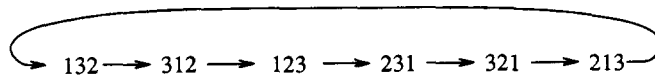


Fig. 4.  $\tilde{G}_3$ .

Finally, if  $x = 6$  then we have  $526 \sim 213$  and  $231 \rightarrow 213$ . So, even after we find a Hamiltonian cycle in  $G_n$ , we still have to assign values  $a_i$  to realize (order-isomorphically) the appropriate elements of  $S_n$ . We will have more to say about this latter. The structure of  $G_3$  can be simplified if we regroup the vertices as in Fig. 4.

We have grouped permutations according to the order type of the first two elements, which are '12' and '21'. An arc in  $\tilde{G}_3$  from 213, for example to the group '12' denotes that there are really *three* arcs, one from 213 to each of the elements 123, 132 and 231 in the group '12'. Since each permutation now has exactly one arc leaving it, it suffices to find an Eulerian circuit in  $\tilde{G}_3$  in order to produce a Hamiltonian circuit in  $G_3$ . We show such an Eulerian circuit for  $\tilde{G}_3$  in Fig. 5. The corresponding Hamiltonian circuit in  $G_3$  is



The key question is now this. How does such a cycle correspond to a  $U$ -cycle for  $S_3$ ?

Suppose we assign (as of yet) undetermined values for the potential  $U$ -cycle as follows:

$$U: a b c d e f.$$

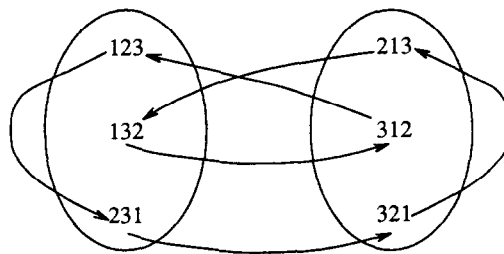


Fig. 5. An Eulerian circuit in  $\tilde{G}_3$ .

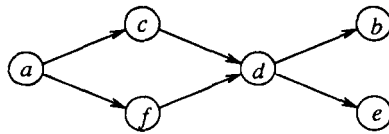


Fig. 6.  $P_3$ .

We want the first 3-block  $abc$  to be order-isomorphic to the first permutation 132 in our Hamiltonian circuit, i.e.,  $abc \sim 132$  which just means  $a < c < b$ . Similarly, we want  $bcd \sim 312$  which implies  $c < d < b$ ,  $cde \sim 123$  which implies  $c < d < e$ , etc.

We can represent the implied inequalities among  $a, b, \dots, f$  by means of a *partial order* (which itself is just an acyclic digraph), where  $i \rightarrow j$  will denote the requirement that  $i < j$ . We show this partial order  $P_3$  in Fig. 6.

What we now require is a mapping of  $\{a, b, \dots, f\}$  into  $\{1, 2, \dots, N\}$  which *preserves order*, i.e., a *linear extension*  $\lambda$  of  $P_3$  into  $\{1, 2, \dots, N\}$  for a suitable

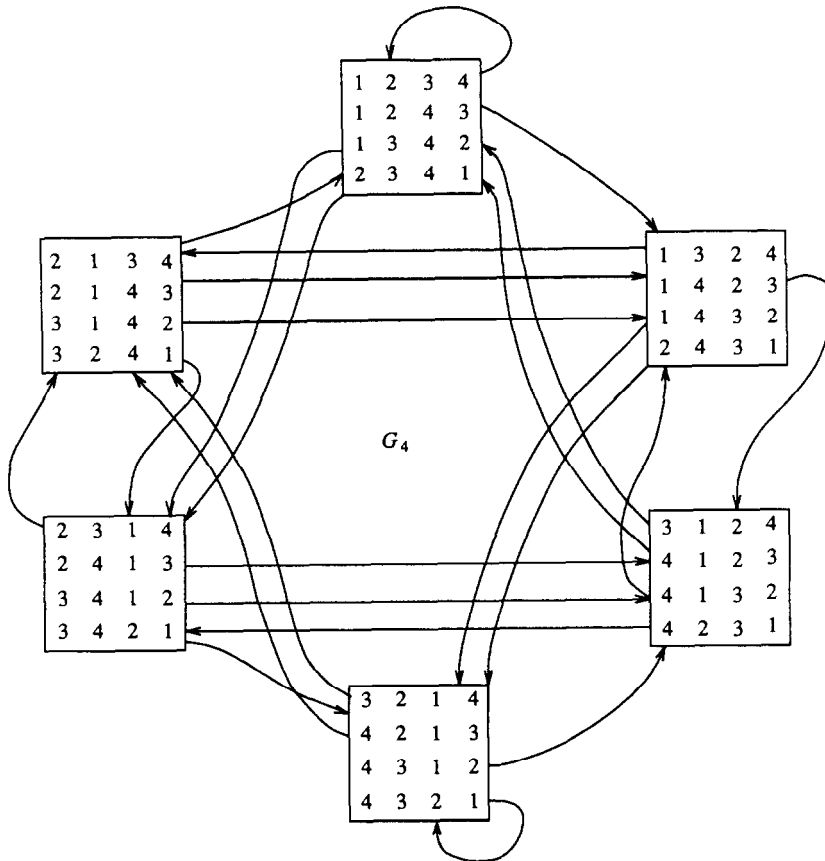


Fig. 7. The clustered transition graph  $\tilde{G}_4$  for  $S_4$ .

$N$ . In particular, it is natural to make  $N$  as small as possible (so that in particular the mapping should be onto). In this case, we can choose  $N=4$  and take  $\lambda(a)=1, \lambda(c)=\lambda(f)=2, \lambda(d)=3, \lambda(b)=\lambda(e)=4$ , which results in the  $U$ -cycle  $142342$  for  $S_3$ .

In Fig. 7 we show the ‘clustered’ transition graph  $\tilde{G}_4$  for  $S_4$ . A particularly nice Eulerian circuit for  $\tilde{G}_4$  is given in Fig. 8.

If we assume that  $U_4 = abc \cdots x$  is a  $U$ -cycle which realizes this ordering of  $S_4$  then we can construct as we did for  $S_3$  the implied partial order  $P_4$  (shown in Fig. 8). This we show in Fig. 9.

The main point is that  $P_4$  has height (= length of longest chain) 5. Thus, we can define the linear extension  $\lambda: \{a, \dots, x\} \rightarrow \{1, 2, 3, 4, 5\}$  by  $\lambda(z) :=$  length of longest chain ending in  $z$ , to produce the  $U$ -cycle

$$1\ 2\ 3\ 4\ 1\ 2\ 5\ 3\ 4\ 1\ 5\ 3\ 2\ 1\ 4\ 5\ 3\ 2\ 4\ 1\ 3\ 2\ 5\ 4.$$

In general, we can cluster vertices of the transition graph  $G_n$  to form  $\tilde{G}_n$  (by grouping together those  $n$  permutations for which the initial  $(n-1)$  blocks are order-isomorphic), which is easily checked to be balanced and strongly connected, and hence Eulerian. It is shown in Hurlbert [10] that by appropriately

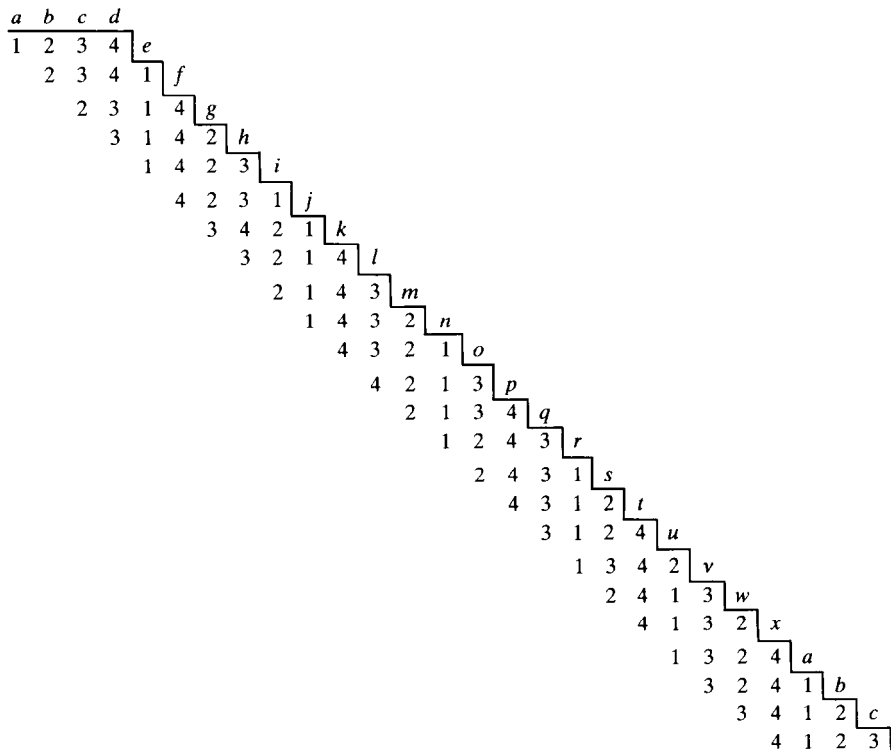


Fig. 8. An Eulerian circuit for  $\tilde{G}_4$ .



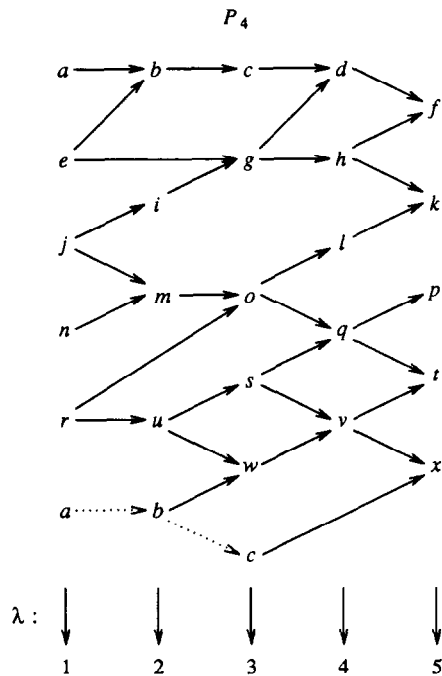


Fig. 9. A linear extension.

restricting  $C$ , the implied ordering on the values in the ‘lifted’  $U$ -cycle is in fact a partial order  $P_n = P_n(C)$ , i.e., has no cycles. (In fact, we believe this to be the case for *any* Eulerian circuit  $C$ .) If  $h(P_n)$  denotes the height of  $P_n$  then there is a linear extension of  $P_n$  into  $\{1, 2, \dots, h(P_n)\}$ , and consequently there is a  $U$ -cycle for  $S_n$  from symbols in  $\{1, 2, \dots, h(P_n)\}$ .

Suppose we define  $N(n) := \min_C h(P_n(C))$  where  $C$  ranges over all Eulerian circuits in  $\tilde{G}_n$ . Then any  $U$ -cycle for  $S_n$  must use at least  $N(n)$  different symbols. The best bounds we currently have for  $N(n)$  are

$$N(2) = 2, \quad N(3) = 4, \quad N(4) = 5 \quad \text{and} \quad n + 1 \leq N(n) \leq 6n \quad \text{for} \quad n \geq 5.$$

However, we believe the following.

**Conjecture.**  $N(n) = n + 1, n \geq 3$ .

We close this section with several questions. How many  $U$ -cycles for  $S_n$  are there with exactly  $N(n)$  different vertices? What about with at most  $N(n) + c$  entries for a fixed constant  $c$ ? Exponentially many? Can we find  $U$ -cycles which are easy to invert? Suppose we just want a specified subset  $X \subseteq S_n$  to be represented by  $U_n$ . For which  $X$  is this possible?

$\underbrace{\left\{ \begin{matrix} 4 \\ 1 \end{matrix} \right\}} = 1$	$\underbrace{\left\{ \begin{matrix} 4 \\ 2 \end{matrix} \right\}} = 7$	$\underbrace{\left\{ \begin{matrix} 4 \\ 3 \end{matrix} \right\}} = 6$	$\underbrace{\left\{ \begin{matrix} 4 \\ 4 \end{matrix} \right\}} = 1$
1234	1   234 2   134 3   124 4   123 12   34 13   24 14   23	1   2   34 1   3   24 1   4   23 2   3   14 2   4   13 3   4   12	1   2   3   4

Fig. 10. Partitions of  $\{1, 2, 3, 4\}$ ,  $U_4: abc b c c c d d c d e e c$ .

**5. Partitions**

The next class of objects we consider is the set of  $P_n$  of *partitions* of the  $n$ -element set  $\{1, 2, \dots, n\}$ . The number of such partitions is just  $\sum_{k=1}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ , where  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$  denotes the Stirling number of the second kind, and satisfies the recurrence

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\} + \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\}$$

(e.g., see [8]).

How will we represent partitions? We will do the following. We illustrate the idea for  $n = 8$ . A  $U$ -cycle for  $P_n$  will be a sequence composed of symbols from the set  $A = \{a, b, c, \dots\}$ . A block, for example,  $abc b c c d$ , will represent a partition, in this case  $13 | 25 | 467 | 8$ , by putting  $i$  and  $j$  in the same group of the partition if and only if the  $i$ th and  $j$ th symbols of the block are the same. In Fig. 10, we list the 15 partitions of  $\{1, 2, 3, 4\}$  and a  $U$ -cycle  $U_4$  for  $P_4$ .

We can proceed in the canonical way in searching for  $U$ -cycles by first considering the corresponding transition graph  $G_n$ . In Fig. 11(a) we show  $G_3$ . In Fig. 11(b) we redraw  $G_3$  by clustering certain partitions together as shown, to form  $\bar{G}_3$ .

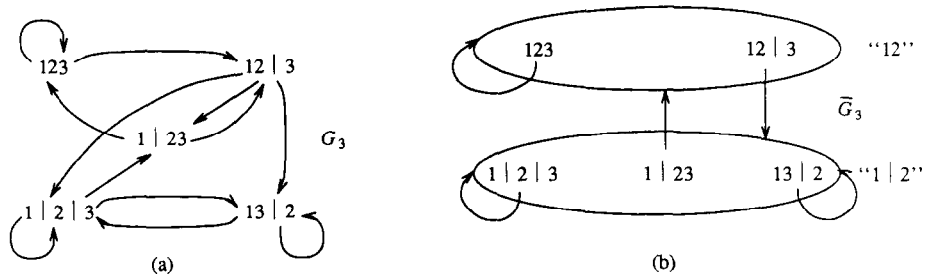
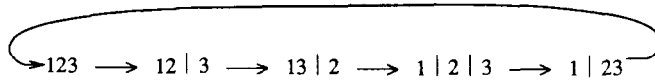


Fig. 11. The graphs  $G_3$  and  $\bar{G}_3$ .

$$\begin{array}{rcccl}
 ? U_4 : & \underline{x_1} & \underline{x_2} & \underline{x_3} & \underline{x_4} & \underline{x_5} \\
 & 1 & 2 & 3 & & \\
 & & 1 & 2 & | & 3 \\
 & & & 1 & 3 & | & 2 \\
 & & & & 1 & | & 2 & | & 3 \\
 & & & & & 1 & | & 2 & 3
 \end{array}
 \quad \begin{array}{l}
 \Rightarrow x_1 = x_2 = x_3 \\
 \Rightarrow x_4 \neq x_3 \\
 \Rightarrow x_5 = x_3 \\
 \Rightarrow x_1 \neq x_5
 \end{array}$$

Fig. 12.

We use the same convention as in the preceding section, namely, an arc from a partition  $\pi$  to a cluster means that arcs go from  $\pi$  to *all* partitions of the cluster. This reduced graph  $\tilde{G}_3$  is Eulerian, with the only Eulerian circuit being



The final step is to ‘lift’ this circuit to an actual  $U$ -cycle by assigning appropriate symbols in order to realize the corresponding partitions. We show the set-up in Fig. 12.

However, we now get a contradiction since we can deduce  $x_5 \neq x_1 = x_3 = x_5$ . Thus, we have an example of a Hamiltonian circuit in  $G_n$  which cannot be ‘lifted’ to a  $U$ -cycle. In fact, there are no  $U$ -cycles for  $P_3$ .

Undaunted, we move on to  $P_4$ . In Fig. 13, we show  $\tilde{G}_4$ .

As before, if we imagine contracting clusters to points, this graph is Eulerian. The reader may wish to test his or her understanding up to this point by finding an Eulerian circuit in  $\tilde{G}_4$  and extending it to a  $U$ -cycle for  $P_4$  (there is more than one way to do this).

For the general case of  $P_n$ , this procedure works quite well. It is not difficult to see that the clustered graph  $\tilde{G}_n$  is always Eulerian (for  $n \geq 3$ ). The only problem we have to worry about is that some Eulerian circuits might not be able to be converted to  $U$ -cycles. This can only happen if the implied (in)equalities in the symbols of the  $U$ -cycle end up with forcing  $x \neq x$  for some symbol  $x$  (as happened for  $n = 3$ ). To prevent this, it is enough to require that a specific sequence  $W$  of partitions occur in the Eulerian circuit  $C$ . The purpose of  $W$  is to prevent a sequence of equalities (or inequalities) from going across the corresponding portion of the  $U$ -cycle. For example, take  $n = 4$  and let  $W$  be

$$1 | 23 | 4, \quad 12 | 34, \quad 1 | 234, \quad 1234, \quad 123 | 4.$$

When this portion of  $C$  is ‘lifted’ we get the situation shown in Fig. 14. Thus, we must have

$$a_{i+1} \neq a_{i+2} = a_{i+3} \neq a_{i+5} = a_{i+6} = a_{i+7} \neq a_{i+8}.$$

We can think of  $W$  as a ‘breaker’ since if  $r \leq i$  and  $s \geq i + 8$  then neither  $a_r = a_s$  nor  $a_r \neq a_s$  can be forced. In particular, if  $C$  has a ‘breaker’ which does not

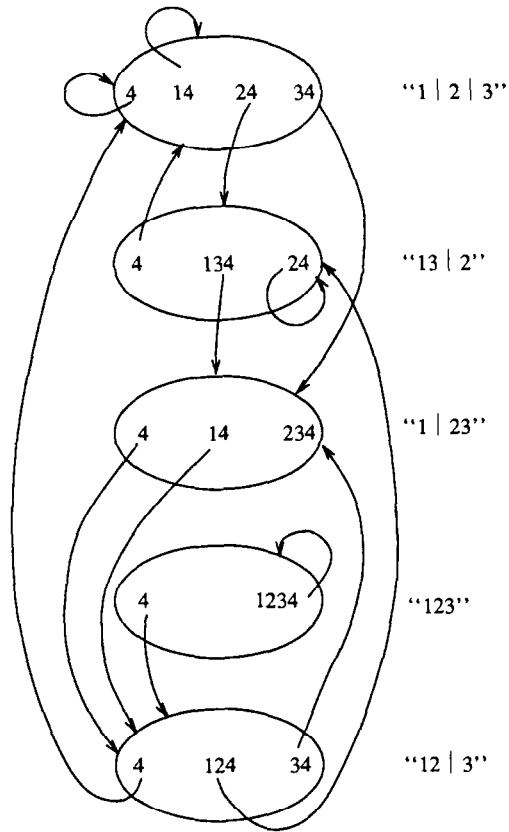


Fig. 13. The reduced graph  $\tilde{G}_4$ .

include  $1 | 2 | 3 | 4$  then  $C$  can always be lifted to a  $U$ -cycle. It is not difficult to show that for  $n \geq 4$  this can always be done.

It is amusing to note that there are exactly 52 partitions of  $\{1, 2, 3, 4, 5\}$ . In fact, a  $U$ -cycle for  $P_5$  can be constructed with the alphabet  $A = \{D, C, H, S, J\}$  so that the symbol  $J$  occurs just once, and each of the other symbols occur at most 13 times. For example, one such cycle is

*DDDDCHHHCCDDCCCHCHCSHHSDDSSSHSDDCHSSCHSHDHSCHSJCDC.*

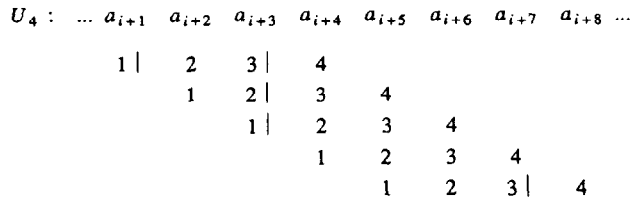


Fig. 14.

In particular, this cycle can be realized with an ordinary deck of playing cards with one spade (=  $S$ ) replaced by a joker (=  $J$ ). It is not hard to see that for  $P_n$ , we must have an alphabet  $|A| \geq n$ . For  $N \geq n$ , how many  $U$ -cycles for  $P_n$  are there with  $|A| = N$ ? How do you invert *any* of these  $U$ -cycles?

**6.  $k$ -Sets of an  $n$ -set**

The final class of objects we consider is the family  $\binom{n}{k}$  of all  $k$ -element subsets (=  $k$ -sets) of an  $n$ -element set  $\{0, 1, \dots, n - 1\}$ . As an example of a  $U$ -cycle for this situation, we have for  $n = 8, k = 3$ , the following cycle  $U$ :

02456145712361246703671345034601250135672560234723570147.

A distinguishing feature of this situation is that each 3-set might occur in any of 6 possible orders in  $U$ , but it is only allowed to occur once. That is, since the first 3-block 024 represents the 3-set  $\{0, 2, 4\}$  then none of the five other 3-blocks 042, 204, 240, 402 and 420 can occur in  $U$ . One consequence of this fact is that we cannot even define a transition graph  $G$  for  $\binom{n}{k}$ ! For if  $\{1, 2, 3\}$  is represented by the block 123, for example, then the arc  $\{1, 2, 3\} \rightarrow \{2, 3, 4\}$  is possible in  $G$  (by having the block continue 1234  $\dots$ ). However, if  $\{1, 2, 3\}$  is represented by 213 then  $\{1, 2, 3\} \rightarrow \{2, 3, 4\}$  cannot be an arc in  $G$ . Since we do not know which way  $\{1, 2, 3\}$  will be represented then we cannot give a meaningful definition of  $G$ .

There is a simple modular condition which is *necessary* for the existence of  $U$ -cycles for  $\binom{n}{k}$ .

**Fact.** *If  $\binom{n}{k}$  has a  $U$ -cycle then  $k$  divides  $\binom{n-1}{k-1}$ .*

**Proof.** Consider a fixed symbol  $a_i = x$  in a  $U$ -cycle  $C$ . Since all symbols  $a_{i+j}, -k < j < k$ , must be distinct from  $x$ , then each copy of  $x$  occurs in exactly  $k$   $k$ -blocks of  $C$ . Since these  $k$ -blocks represent  $k$ -sets of  $\{0, \dots, n - 1\}$  which contain  $x$ , and there are exactly  $\binom{n-1}{k-1}$  if these, the conclusion follows.  $\square$

It is easy to see that  $U$ -cycles exist for  $\binom{n}{2}$  whenever this necessary condition is satisfied, i.e.,  $n$  is odd.

It has been shown by Jackson [12] that this necessary condition is in fact sufficient for  $k = 3$  if  $n$  is large enough.

**Theorem** [12].  *$U$ -cycles exist for  $\binom{n}{3}$ ,  $n \geq 8$ , provided  $\binom{n-1}{2} \equiv 0 \pmod{3}$ .*

**Idea of proof.** We illustrate the idea for  $n = 8$ . We first tabulate all possible different ways of selecting 3 elements from an 8-cycle where we identify two choices if they only differ by a rotation. We describe these by their sequences of differences between consecutive elements (modulo 8) (see Fig. 15). We next

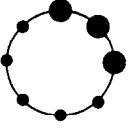
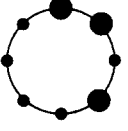
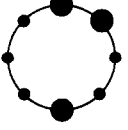
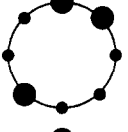
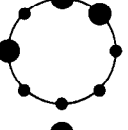
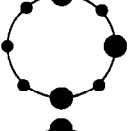
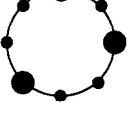
<u>PATTERN</u>	<u>DIFFERENCES (mod 8)</u>
	<u>1 1 6</u>
	<u>1 2 5</u>
	<u>1 3 4</u>
	<u>3 1 4</u>
	<u>2 1 5</u>
	<u>2 2 4</u>
	<u>3 3 2</u>

Fig. 15. Possible cyclic patterns for 3-sets of an 8-set.

select for each (ordered) pattern *two* of the three differences (underlined in Fig. 15).

Now we construct a digraph  $G$  with vertices labeled by 1, 2 and 3, and arcs from  $i$  to  $j$  if  $ij$  is an (ordered) pair of differences selected in the previous stage. We show  $G$  in Fig. 16.

For the next step we look for an Eulerian circuit  $C$  in  $G$ . In this case we take

$$\left( \overbrace{2 \ 2 \ 1 \ 1 \ 3 \ 3 \ 1} \right).$$

Finally we check that the sum  $\Sigma$  of the elements of  $C$  is relatively prime to  $n = 8$ . Since  $\Sigma = 5$  in this case, then this stage passes. If we have managed to succeed up to this point then we can now construct our  $U$ -cycle  $U$  as follows. We take the

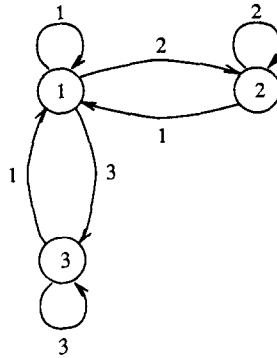


Fig. 16. The graph for 3-sets of an 8-set.

‘template’ of differences 2 2 1 1 3 3 1 2 2 1 1 3 3 1 2 ... and construct the sequence of length  $7 \cdot 8 = 56$  having these differences (mod 8) between consecutive elements. (It does not matter what the first element of  $U$  is). Thus,  $U$  (starting with 0) is

$$\begin{array}{l} \Delta: \quad 2 \ 2 \ 1 \ 1 \ 3 \ 3 \ 1 \ 2 \ 2 \ 1 \ 1 \ 3 \ 3 \ 1 \ 2 \ \dots \\ U: \quad 0 \ 2 \ 4 \ 5 \ 6 \ 1 \ 4 \ 5 \ 7 \ 1 \ 2 \ 3 \ 6 \ 1 \ 2 \ 4 \ \dots \end{array}$$

What Jackson shows is that it is always possible to construct a  $U$ -cycle for  $\left[ \begin{smallmatrix} n \\ 3 \end{smallmatrix} \right]$  this way, provided  $3 \mid \binom{n-1}{2}$ , i.e.,  $n \not\equiv 0 \pmod{3}$ , and  $n \geq 8$ .

These techniques can be extended to show the following.

**Theorem.**  $U$ -cycles exist for  $\left[ \begin{smallmatrix} n \\ 4 \end{smallmatrix} \right]$  provided  $\binom{n-1}{3} \equiv 0 \pmod{4}$ ,  $(n, 4) = 1$  and  $n$  is sufficiently large.

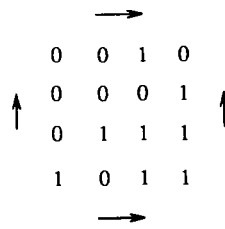
It has very recently been shown by Hurlbert [10] that the necessary condition  $\binom{n-1}{5} \equiv 0 \pmod{6}$  is also sufficient for the existence of  $U$ -cycles for  $\left[ \begin{smallmatrix} n \\ 6 \end{smallmatrix} \right]$ . However, for  $k = 5$  or  $k \geq 7$  we are still completely baffled.

We are willing to make the following conjecture though.

**Conjecture** (\$100).  $U$ -cycles exist for  $\left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]$  always exist provided  $k$  divides  $\binom{n-1}{k-1}$  and  $n \geq n_0(k)$ .

### 7. Future directions

There are of course many other combinatorial structures for which these and similar questions can be raised. Thus include, for example, permutations with ties, ordered  $k$ -sets of an  $n$ -set,  $k$ -sets of an  $n$ -element multi-set,  $k$ -dimensional subspaces of an  $n$ -dimensional vector space over  $\text{GF}(q)$ , combinatorial  $k$ -spaces

Fig. 17. A de Bruijn torus for  $2 \times 2$  arrays.

of an  $n$ -space (a la Hales–Jewett; see [9]), etc. One could also ask for higher-dimensional analogues of these questions. For example, is it always possible to construct a *universal torus*  $T$  for every  $2k$ -by- $2k$  binary array? In other words, we are asking for a (square)  $2^{2k^2}$ -by- $2^{2k^2}$  binary array  $T$ , with horizontal and vertical sides, respectively, identified, so that all  $2k$ -by- $2k$  binary arrays occur in  $T$  exactly once. The simplest example of such a  $T$  is shown in Fig. 17. In fact, such  $T$  always exist (see [6]) although their number for each size is not known.

Non-square toruses have been investigated in [2–4, 7, 11, 16, 18–19], and in particular in [20], where they arise in connection with robot self-location problems.

Clearly we have barely scratched the surface of this subject, with the vast bulk of the interesting results remaining yet to be discovered. An excellent start in some of these directions can be found in [10].

## References

- [1] N.G. de Bruijn, A combinatorial problem, Proc. Nederl. Akad. Wetensch. 49 (1946) 758–764.
- [2] C.R.J. Clapham, Universal tilings and universal  $(0, 1)$ -matrices, Discrete Math. 58 (1986) 87–92.
- [3] J.C. Cook, Toroidal tilings from de Bruijn—Good cyclic sequences, Discrete Math. 70 (1988) 209–210.
- [4] K. Dehnhardt and H. Harborth, Universal tilings of the plane by 0–1 matrices, Discrete Math. 73 (1988/89) 65–70.
- [5] H. Fredericksen, A survey of full length nonlinear shift register cycle algorithms, SIAM Rev. 24 (1982) 195–221.
- [6] C.T. Fan, S.M. Fan, S.L. Ma and M.K. Sin, On de Bruijn arrays, Ars Combin. 19A (1985) 205–213.
- [7] B. Gordon, On the existence of perfect maps, IEEE Trans. Inform. Theory 12 (1966) 486–487.
- [8] R.L. Graham, D.E. Knuth and O. Patashnik, Concrete Mathematics (Addison-Wesley, Reading, MA, 1989).
- [9] R.L. Graham, B.L. Rothschild and J.H. Spencer, Ramsey Theory (Wiley, New York, 1980).
- [10] G. Hurlbert, Ph.D. Thesis, Rutgers Univ., 1990.
- [11] A. Iványi, Construction of infinite de Bruijn arrays, Discrete Appl. Math. 22 (1988/89) 289–293.
- [12] Brad Jackson, personal communication.
- [13] D.E. Knuth, Oriented subtrees of an arc digraph, J. Combin. Theory 3 (1967) 309–314.
- [14] D.E. Knuth, Fundamental Algorithms, The Art of Computer Programming, Vol. 1 (Addison-Wesley, Reading, MA, 2nd ed., 1973) 371–381, 576–581.
- [15] A. Lempel,  $m$ -Ary closed sequences, J. Combin. Theory 10 (1971) 253–258.



- [16] J.H. van Lint, F.J. MacWilliams and N.J.A. Sloane, On pseudo-random arrays, *SIAM J. Appl. Math.* 36 (1979) 62–72.
- [17] M.H. Martin, A problem in arrangements, *Bull. Amer. Math. Soc.* 40 (1934) 859–864.
- [18] F.J. MacWilliams and N.J.A. Sloane, Pseudo-random sequences and arrays, *Proc. IEEE* 64 (1976) 1715–1729.
- [19] T. Normura, H. Miyakawa, H. Imai and A. Fukuda, A theory of two-dimensional linear arrays, *IEEE Trans. Inform. Theory* 18 (1972) 775–785.
- [20] F.W. Sinden, Sliding window codes, AT&T Bell Labs Tech. Memorandum, 1985.
- [21] S. Stein, The mathematician as an explorer, *Sci. Amer.* May (1961) 149–158.
- [22] M. Yoeli, Binary ring sequences, *Amer. Math. Monthly* 69 (1962) 852–855.