Products of Universal Cycles

Persi Diaconis [*][†]   Ron Graham [‡][§]

Abstract

Universal cycles are generalizations of de Bruijn cycles to combinatorial patterns other than binary strings. We show how to construct a **product cycle** of two universal cycles, where the window widths of the two cycles may be different. Applications to card tricks are suggested.

1 Introduction

A de Bruijn cycle is a sequence of zeros and ones such that each window of width k running along the sequence shows a different binary k-tuple. We assume the ends of the sequence are joined to form a cycle. For example, when $k = 3$,

$$1\,0\,1\,1\,1\,0\,0\,0$$

shows $101, 011, 111, 110, 100, 000, 001, 010$ (where the window is run "around the corner"). In this example, the total length of the cycle is $2^3 = 8$, so each 3-tuple appears once. We do not require this, so that $0\,0\,0\,1\,1\,1$ (for $k = 3$) is a de Bruijn cycle of length six. The reader may enjoy the problem of constructing a de Bruijn cycle of length 52 for a window of width $k = 6$.

De Bruijn cycles are used for cryptography, robot vision, random number generation and DNA sequencing. In [2], we show they can be used secretly for card tricks. A friendly introduction to de Bruijn sequences is in Stein [15]; a more comprehensive survey is in Fredericksen [4]; see Knuth [13] for an extensive discussion. These articles show that maximal length de Bruijn sequences always

[*] Stanford University, Stanford, CA 94305

[†] Research supported in part by NSF Grant DMS 0505673

[‡] University of California at San Diego, San Diego, CA 92093

[§] Research supported in part by NSF Grant CCR-0310991

exist for any window width k. They give a variety of constructions and properties (for example, they show how to determine the binary pattern in position t). It is even known exactly how many maximal length de Bruijn sequences there are: $2^{2^{k-1}-k}$.

In joint work with Fan Chung [1], we have introduced a generalization called "universal cycles" which extend the notion from binary strings to other combinatorial patterns such as the relative order of k consecutive symbols. Thus, consider for window width 3, the sequence

$$1\,3\,2\,1\,3\,4.$$

The relative order of the first three numbers is **Low-High-Medium** or **LHM**. The successive relative orders (going around the corner) are:

LHM, **HML**, **MLH**, **LMH**, **MHL**, **HLM**.

Thus, each of the six possible relative orders (or permutations) appears exactly once. This is an example of a universal cycle for permutations. In our work with Chung, we showed that for every k, the numbers $1, 2, 3, \dots, k!$ can be arranged so that each consecutive block of k has a distinct relative order. While such sequences were shown to exist, no general rule for construction, nor any formula (or approximation) for the total number is known. The reader may enjoy one of the following two problems:

- Write the numbers $1, 2, 3, \dots, 24$ in a sequence so that each successive group of **four** shows a distinct relative order.

- Write down a sequence of length 24 using only the numbers $1, 2, 3, 4, 5$ so that each successive group of **four** shows a distinct relative order.

We have also constructed sequences of symbols $1, 2, \dots, n$ so that each consecutive k-tuple shows a distinct k-subset from the set $\{1, 2, \dots, n\}$. These only exist for certain k and n; here even the existence is an open research problem. This is a universal cycle for k-subsets of an n-set. See Jackson [11] and Hurlbert [8] for more details.

More generally, given any natural combinatorial object described by k parameters $(\theta_1, \theta_2, \ldots, \theta_k)$, one may ask for a sequence of θ-values so that each consecutive block of k codes exactly one of our objects. More carefully, there is a fixed finite alphabet Θ, and each θ_i is in Θ. Further, there is a rule $R(\theta_1, \theta_2, \ldots, \theta_k)$ taking values **one** or **zero**. Our combinatorial object is the set of all $(\theta_1, \theta_2, \ldots, \theta_k)$ so that $R(\theta_1, \theta_2, \ldots, \theta_k) = 1$. For example, if $\Theta = \{1, 2, \ldots, k\}$ and $R(\theta_1, \theta_2, \ldots, \theta_k)$ is one if the θ_i are distinct, and zero otherwise, then the combinatorial object is the set of all permutations on k symbols.

A variety of constructions have appeared: set partitions, ordered k-out-of-n, subspaces of a vector space, and others. It seems fair to say that up to now, the construction of universal cycles has proceeded by clever, hard, ad-hoc arguments. There is nothing like a general theory.

The purpose of the present article is to begin a theory by showing that for some cases, **products** of universal cycles can be formed. In the next section, we introduce the product construction by taking the product of 1 0 1 1 1 0 0 0 and 1 3 2 1 3 4. A card trick version version is given along with a general recipe for the product of a de Bruijn cycle and an arbitrary universal cycle — both with the same window width k. The following section gives products for universal cycles more general than de Bruijn cycles with an arbitrary universal cycle, and which have (possibly) differing window widths. Following this is a practical section which concerns "cutting down" universal cycles (e.g., from 64 to 52). Proofs are deferred to the Appendix, which gives a very general product construction.

2 Products with Equal Window Widths

Suppose that $x_1\, x_2 \ldots x_R$ and $y_1\, y_2 \ldots y_S$ are each universal cycles for the same window width k. We want to use these to form a sequence of **pairs**

$$\begin{array}{cccc} x_1 & x_2 & \ldots & x_{RS} \\ y_1 & y_2 & \cdots & y_{RS} \end{array}$$

so that a window of width k, run along the pairs, shows each of the possible (vertical) pairs of x-tuples and y-tuples just once. The easiest case occurs when the integers R and S have no common factor larger than 1. We may then simply write $x_1 x_2 \ldots x_R x_1 x_2 \ldots x_R \ldots x_1 x_2 \ldots x_R$, repeated S times. Under this, write $y_1 y_2 \ldots y_S y_1 y_2 \ldots y_S \ldots y_1 y_2 \ldots y_S$ repeated R times.

Example 1: $R = 3$, $S = 4$, $k = 2$

Let the x-sequence code relative order with ties permitted. Thus, two successive values may be **Low-High (LH)** or **High-Low (HL)** or **Equal (EQ)**. Thus, the sequence 112 gives **EQ, LH, HL** (where the last pair comes from going around the corner). The y-sequence uses zeros and ones, such as 0011, for the usual de Bruijn sequence for window width $k = 2$. Here, $RS = 12$. The product is

$$\begin{array}{cccccccccccc} 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array}$$

Our interest in forming products arose from a card trick. We wanted to take a product of the usual de Bruijn sequence 1 0 1 1 1 0 0 0 of length eight with the permutation sequence 1 3 2 1 3 4 of length six. Both have window width $k = 3$. This would give an arrangement of 48 cards so that the relative order and color pattern of successive triples uniquely determines the position. We originally constructed an example in an ad hoc fashion (the naïve construction above doesn't work since $R = 6$ and $S = 8$ are not relatively prime). We then developed some theory (described below). Here is the construction that the theory gives:

Take an ordinary deck of cards. Remove the four Kings. Arrange the rest in the order (Ace is low), with D, C, H, S for Diamonds, Clubs, Hearts and Spades:

$$\begin{array}{cccccccccccccccc} A & 7 & 5 & 3 & 9 & J & 2 & 7 & 6 & 3 & 10 & Q & A & 8 & 5 & 4 \\ D & C & D & H & H & S & C & S & H & S & D & H & H & C & S & C \\ \\ 10 & Q & 2 & 7 & 5 & 3 & 10 & J & A & 8 & 6 & 4 & 10 & J & 2 & 8 \\ H & S & D & D & H & C & S & H & C & H & D & D & C & C & S & D \\ \\ 6 & 4 & 9 & J & A & 8 & 6 & 3 & 9 & Q & 2 & 7 & 5 & 4 & 9 & Q \\ C & H & D & D & S & S & S & D & C & D & H & H & C & S & S & C \end{array}$$

The reader will find that each successive group of three cards is uniquely identified by the relative order and color pattern. For example, the top three cards are AD, $7C$, $5D$ and have relative order L, H, M and color pattern R, B, R. No other successive triple has both of these patterns. This property can be used to perform a card trick. Put the 48-card deck, arranged as above, in the card case. Find an audience, the larger, the better. Have the audience members take the cased deck and pass it to the back of the hall. Have a "randomly chosen spectator" cut the deck and complete the cut. The deck is passed to a second, adjacent, spectator who also gives the cards a complete cut. Then, the deck is passed to a third spectator who gives it a complete cut. This third spectator removes the current top card, showing it to no one. The deck is passed back to the second spectator who removes the top card and then back to the first spectator who removes the top card. The performer patters as follows:

"Three of you have freely cut the cards and selected a card. I'd like you to look at your card and concentrate, form a mental picture and try to project. You're doing a great job, but it's hard to unscramble things. Let me try this. I see Red more clearly than Black. Would everyone with a Red card please stand up? That helps a lot! But still, it's not in focus; Who has the highest card of you three". (One of the spectators waves.) *"Who has the lowest?".* (Again, one of the spectators waves.) *"I'll work on the middle man first. You, sir, have a Spade,…, it's the nine of Spades? Now, the high man; You have a high Black card; is it the Queen of Clubs? Finally, the lady with the lowest card. It's a four. Is it the four of Spades?".*

Practical performance details for tricks of this type are in [2], Chap. 2. We mention the magic application to explain our motivation for the constructions in the present paper.

The 48-card arrangement was constructed in two stages. First, we used the product theorem described below to get a "product" of the universal cycle for permutations (namely, 1 3 2 1 3 4) with the de Bruijn cycle (namely, 10111000). This results in the following sequence of 48 pairs:

1	3	2	1	3	4	1	3	2	1	3	4	1	3	2	1	3	4	1	3	2	1	3	4
1	0	1	1	1	0	0	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	0	1

1	3	2	1	3	4	1	3	2	1	3	4	1	3	2	1	3	4	1	3	2	1	3	4
0	1	1	1	0	0	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	0	0	0

Notice that the bottom row is not quite a repetition of 1 0 1 1 1 0 0 0. Nonetheless, the product theorem guarantees that each three successive pairs are uniquely determined by the relative order of the top sequence and the zero-one pattern of the bottom sequence.

The second stage requires lifting the last pattern to the natural context of playing cards with twelve values, each repeated four times, and four suits. We explain how to lift in Section 4.2 below. We now state a first product theorem.

Theorem 1. (Product of a de Bruijn and universal cycle with equal window lengths).

Let $\overline{x} = x_1 x_2 \dots x_R$ be an arbitrary universal cycle with window width k. Let $\overline{y} = y_1 y_2 \dots y_S$ be a de Bruijn cycle with window width k. Here, the symbols x_i can be in any alphabet, the symbols y_j are zero-one. Neither cycle need be maximal, but we do assume that $\overline{y}$ ends with k consecutive zeros. The following construction gives a sequence of pairs $\begin{matrix} x_i \\ y_j \end{matrix}$ of length RS so that if a window of width k is run along the pairs, each ordered k-tuple of x_i's above an ordered k-tuple of y_j's appears just once.

Construction. If the sequence lengths R and S have no common factor, repeat the $\overline{x}$-sequence S times above the $\overline{y}$-sequence repeated R times. If the largest number that divides R and S is d, write $R = rd$ and $S = sd$. Observe that r and s are relatively prime. Begin by writing down the $\overline{x}$-sequence S times, forming a sequence of length RS. Under this, we construct the following sequence. Recall that $\overline{y}$ is a de Bruijn sequence with k zeros at the end. Form a string of zeros and ones by repeating the original sequence $\overline{y}$ a total of r times, and then removing the final zero. This gives a sequence $\overline{y}^*$ of length $rS - 1$. Now, repeat the $\overline{y}^*$

sequence d times, and finish off with a string of d zeros. Place this, in order, under the $\overline{x}$-sequence of length RS.

Example 2. Look back at the product of $1\,3\,2\,1\,3\,4$ and $1\,0\,1\,1\,1\,0\,0\,0$ in the preceding section. Here, $R = 6$, $S = 8$, and so the greatest divisor is $d = 2$. The construction begins by repeating $1\,3\,2\,1\,3\,4$ eight times to form the top row. For the bottom row, $r = 3$. The block $\overline{y}^*$ is formed from three copies of $1\,0\,1\,1\,1\,0\,0\,0$ and then deleting the final zero. Thus, $\overline{y}^* = 1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0$. The bottom row is formed from $d = 2$ copies of $\overline{y}^*$ followed by $d = 2$ further zeros.

Example 3. Let us take the product of $1\,1\,0\,0$ with itself. Thus, $R = S = d = 4$ and $r = s = 1$. The top sequence is formed from four copies of $1\,1\,0\,0$. For the bottom row, the building block is $\overline{y}^* = 1\,1\,0$. Placing four repetitions of this followed by four final zeros gives the product sequence:

$$\begin{array}{cccccccccccccccc}
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}$$

The reader may check that the sixteen 2 × 2 windows are distinct:

$$\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \quad \begin{array}{cc} 1 & 0 \\ 1 & 0 \end{array} \quad \begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array} \quad \begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array} \quad \begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array} \quad \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \quad \begin{array}{cc} 0 & 0 \\ 1 & 1 \end{array} \quad \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}$$

$$\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \quad \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \quad \begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array} \quad \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \quad \begin{array}{cc} 1 & 1 \\ 0 & 0 \end{array} \quad \begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \quad \begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \quad \begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array}$$

Example 4. Of course, our product construction can be iterated. Consider the extreme case of $k = 1$. A de Bruijn cycle for $k = 1$ is $1\,0$. The product of this with itself (using the product theorem) is:

$$\begin{array}{cccc}
1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0
\end{array}$$

We may now take the product of this with 1 0 to get:

$$\begin{array}{cccccccc}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}$$

Another product with 1 0 gives:

$$\begin{array}{cccccccccccccccc}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0
\end{array}$$

Can the reader see the simple pattern and how it will continue? (Hint: read the columns upside-down and backwards, in binary.)

We conclude this section with a few remarks which extend the construction in various ways.

Remarks. The construction given was for $\overline{y}$, a zero-one de Bruijn sequence. This is not at all required. The construction works for **any** universal cycle with window width k that contains a block of k repeated symbols. We will call such universal cycles **special.** Here are several other such examples.

Example 5. In [1] we give a universal cycle for partitions of an n-element set. These partitions are counted by the Bell numbers. Martin Gardner give a wonderful introduction to these numbers in [5] (see also Knuth [14] for some extensions). For example, there are 15 partitions of the 4-element set $\{1, 2, 3, 4\}$:

1234	1|234	12|34	1|2|34	1|2|3|4
	2|134	13|24	1|3|24	
	3|124	14|23	1|4|23	
	4|123		2|3|14	
			2|4|13	
			3|4|12	

A universal cycle for these is 1 2 3 2 3 3 3 3 4 4 3 4 5 5 3. As a window of width four is run along, the equal positions run through all possible set partitions exactly once (so that 1 2 3 2 corresponds to the partition 1|3|24, and 2 3 2 3 corresponds to the partition 13|24, etc). Since there is a block of four repeated symbols, namely 3 3 3 3, these can be cycled to the end, and then the product with any universal cycle can be formed.

Example 6. In [Stanford Tech Report] [3], we give a universal cycle for permutations with ties. For example, there are 13 possible relative orders of 3 distinct values when ties are allowed. They are:

$$123,\ 132,\ 213,\ 231,\ 312,\ 321,\ 112,\ 121,\ 211,\ 221,\ 212,\ 122,\ 111$$

A universal cycle for these permutations of 3 symbols with ties (using the symbols $\{1, 2, 3, 4\}$) is given by 1 1 1 2 1 2 2 1 3 4 1 3 2. Since for any window width k for these universal cycles, there is always a block of k repeated symbols (all k values are tied), then these cycles are special, and can be used in the product theorem.

Alas, not every universal cycle has a block of repeated symbols, and we are at a loss for a general construction. For example, when $k = 3$, with the permutation cycle 1 3 2 1 3 4, we do not know how to form a product of 1 3 2 1 3 4 with itself. However, we can construct a cycle of 36 pairs of numbers so that the relative order of the top and bottom blocks of 3 are all distinct. We just need a little more freedom in the alphabet size. An example of such a cycle is:

$$\begin{array}{cccccccccccccccccc}
1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 \\
1 & 4 & 3 & 2 & 5 & 1 & 4 & 3 & 2 & 5 & 1 & 4 & 3 & 2 & 5 & 1 & 4 & 3 \\
 & & & & & & & & & & & & & & & & & \\
1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 \\
2 & 5 & 1 & 4 & 3 & 2 & 5 & 1 & 4 & 3 & 2 & 5 & 6 & 7 & 8 & 9 & 10 & 11
\end{array}$$

For this sequence, the first block of three is $\begin{matrix}1 & 3 & 2 \\ 1 & 4 & 3\end{matrix}$. The top row is in order **L H M**, and the bottom row is in the same order **L H M**. This is the only time this pair of orders appears together. Similarly, every pair of blocks of three (going around the corner) has a unique signature.

We created this sequence by "lifting" (see Section 4.2 below) 1 3 2 1 3 4 to have all distinct symbols, e.g., 1 4 3 2 5 6. Here, every block of three has a unique relative order. This lifting has the property that it can be "cut down" (see Section 4.1 below) to 1 4 3 2 5. This has every block of three with distinct relative orders, but omits **L M H**. Pasting six copies of this under six copies of our original 1 3 2 1 3 4 leaves six places to fill at the end. We filled them with 6 7 8 9 10 11 to give **L M H** six times with all possible order parameters occurring on top. What is also crucial (and this is the result of "fooling around" and not "higher math") is that the construction works going around the corner. Thus, the last block of two $\begin{matrix}3 & 4\\ 10 & 11\end{matrix}$ combined with the first block of length one $\begin{matrix}1\\ 1\end{matrix}$ gives $\begin{matrix}3 & 4 & 1\\ 10 & 11 & 1\end{matrix}$. On top we have **M H L** and on the bottom **M H L**. This is the only time this occurs. Similarly, $\begin{matrix}4 & 1 & 3\\ 11 & 1 & 4\end{matrix}$ gives **H L M** and **H L M** uniquely. We hope that explaining our construction demystifies it and suggests further ideas for progress in constructing products.

3 More General Products

In the section above, we have explained how to form a product of a universal cycle with a de Bruijn cycle **provided** the two cycles have the same window width k. It turns out that the construction given works even if the window widths are different. As explained below, this generalization can be applied to card tricks in at least two ways. Suppose that $\overline{x} = x_1x_2\dots x_R$ and $\overline{y} = y_1y_2\dots y_S$ are universal cycles of respective window widths k and l. Suppose we can construct a sequence of pairs

$$\begin{matrix}x_1 & x_2 & \dots & x_{RS}\\ y_1 & y_2 & \cdots & y_{RS}\end{matrix}$$

with x_i in the alphabet used for the $\overline{x}$-sequence, and y_j in the alphabet used for the $\overline{y}$-sequence. The construction is a **product** if starting at any position $\begin{matrix}x_i\\ y_i\end{matrix}$, the symbols $x_ix_{i+1}\dots x_{i+k-1}$ and $y_iy_{i+1}\dots y_{i+l-1}$ uniquely identify i.

Here is a simple example. Take $\overline{x} = 1\,3\,2\,1\,3\,4$. With $k = 3$, this is a universal cycle for permutations. Take $\overline{y} = RRWBBRBWW$. With $l = 2$, successive windows of width 2 go through each of the nine ordered pairs of 'colors' $\{Red, White, Blue\}$. The lengths $R = 6$ and $S = 9$ have the largest common factor of $d = 3$. We may follow the construction of the Product Theorem virtually word for word: Build a sequence of total length $RS = 54$ by first repeating

S copies of the $\overline{x}$-sequence. For the second row, $R = rd = 2 \cdot 3$. Repeat the $\overline{y}$-sequence $r = 2$ times and delete the final symbol. This gives $\overline{y}^* = RRWBBRBWWRRWBBRBW$. Next, repeat the $\overline{y}^*$-sequence d times and finish off with d repetitions of the deleted symbol W. This gives the final construction:

$$\begin{array}{cccccccccccccccccc}
1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 \\
R & R & W & B & B & R & B & W & W & R & R & W & B & B & R & B & W & R \\[1em]
1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 \\
R & W & B & B & R & B & W & W & R & R & W & B & B & R & B & W & R & R \\[1em]
1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 2 & 1 & 3 & 4 \\
W & B & B & R & B & W & W & R & R & W & B & B & R & B & W & W & W & W
\end{array}$$

Consider this sequence. The relative order of the first three places is **L H M**. The colors of the first two places are R . The reader may check that this pattern only occurs at the start: The $R\,R$ pattern occurs just six times, and the three symbols directly above occur in six distinct relative orders.

Here are two ways such a product could be used for a card trick. First, suppose $k \geq l$. Have the deck of RS cards cut freely and have k consecutive cards taken off. Each card is representated by a labeled $\begin{matrix} x_i \\ y_i \end{matrix}$ pair. Ask for the $\overline{x}$ information. Then, ask the first l people for the $\overline{y}$ information. This combined information uniquely identifies the k cards. Here is a second procedure. Have $k + l$ cards taken off. Ask the first k people for the $\overline{x}$ information and the last l people for the $\overline{y}$ information. This information uniquely specifies the cards.

As a check, the reader may try both procedures out on the sequence of length 54 given above.

Combining techniques, we have a way of taking a product of two universal cycles, one of window width k and one of window width l, provided only that at least one of the two cycles contains a window of all identical symbols (or that the lengths of the two cycles are relatively prime). Neither cycle need be maximal or de Bruijn. We call this the **General Product Construction** (Theorem 3). The validity of the construction described and somewhat more will be proved in the Appendix. Of course, higher order products can be constructed by iterating the procedure.

4 Some Practical Details and Problems.

Over the years of working with de Bruijn sequences and their generalizations, four practical problems have emerged. These are:

- Products
- Cutting down
- Lifting/lumping
- Coding and neat generation

We have treated products earlier. We briefly treat the three remaining problems here.

4.1 Cutting Down

Maximal length universal cycles come in tightly circumscribed lengths. For binary de Bruijn sequences, these lengths are $2, 4, 8, 16, 32, 64, \ldots$. Practical considerations may demand a shorter total length. For example, 52 is boxed between 32 and 64. We know there are maximal length de Bruijn sequences of length 32 (window width 5) and 64 (window length 6). What do we know for 52? One approach would be to take a de Bruijn sequence of length 64 and cut it down. Remove segments of total length 12 so that the remaining 52 show all distinct patterns when a window of width six is run along the cycle. With patience, the reader will find that this is indeed possible. However, there is a very beautiful method for accomplishing this for **any** cycle length in **any** longer maximal de Bruijn cycle. While we would love to take credit for this, it actually belongs to the 'folklore' of de Bruijn cycles (we thank Hal Fredericksen and Al Hales for tracking this down for us). We have it catalogued as "Babai's Cutting Down Lemma". It gives a way of taking a de Bruijn sequence created from a 'shift register' of total length $2^k - 1$ (window width k) and cutting down

to **any** length L, $\quad k \leq L \leq 2^k - 1$. We will illustrate this with the example $k = 6$, $2^k - 1 = 63$, and $L = 52$.
First, consider the long de Bruijn sequence (length 63):

$$0000010000|1100010100|1111010001|1100100101|1011101100|1101010111|111$$

where we have put |'s after every ten symbols to help count. Label the positions starting at the extreme left (position zero) to the extreme right (position 62). For example, the window of width six that starts at position 38 is 011011. The window starting at position 49 is 011010. These will figure into the discussion in a moment. As with any de Bruijn sequence, a window of width six run along the sequence shows all distinct blocks (except 000000 which does not occur in sequences generated by shift registers).

The sequence is formed from the starting block 000001 by a simple rule: Form the symbol at position $i + 6$ by adding the two symbols at positions i and $i + 1$ (mod 2). Any of the articles cited in our bibliography show how to find such rules and their relation to the algebraic fact the $1 + x + x^6$ is a "primitive" polynomial.

To get from 63 to 52, we must remove 11 symbols. Note that $49 - 38 = 11$, and that the blocks starting at 38 and 49 differ in their last symbol only. We may thus simply replace the last symbol (a 1) in the 38 block 0 1 1 0 1 1 by a zero, cut out the intervening symbols and get:

$$0000010000|1100010100|1111010001|1100100101|1010101111|11$$

The point of this construction (other than that it works) is this: the cut down sequence of length 52 is **still** generated by a simple rule. Consider any block of length six. The next symbol after a block of six is formed by adding the first two symbols of the block (mod 2) **unless** the string formed from symbols two through seven would become 0 1 1 0 1 1. In that case, and in that case only, the simple rule is broken and a zero is adjoined instead, forming the block 0 1 1 0 1 0. This can happen at most once.

We claim that for any window width k and any cut down size, the same scheme works with just one forbidden sequence. To see why (briefly), let $P(x)$ by the primitive polynomial generating your de Bruijn sequence. Our references show that the symbols are generated by raising x to successive powers $x, x^2, x^3, x^4, \ldots \pmod{P(x)}$. If we seek to cut out a chunk of length c (in our case, $c = 11$), we need a power i so that

$$x^{i+c} + x^i \equiv 1 \pmod{P(x)} \quad \text{or} \quad x^i(x^c + 1) \equiv 1 \pmod{P(x)}$$

Because the non-zero elements mod $P(x)$ form a field, this equation always has a unique solution for i, as long as $c \neq 2^k$. The string coded by x^i begins at 38 in our example. All of this will be Greek to the reader who does now know about finite fields; we hope it induces some to learn more!

Two final remarks. First, finding the i that works must be done by trial and error (it is equivalent to finding logarithms in finite fields). Second, the procedure can be written as a simple "nonlinear" recurrence. In the example,

$$x_{n+6} \equiv x_n + x_{n+1} + \overline{x}_n x_{n+1} x_{n+2} \overline{x}_{n+3} x_{n+4} x_{n+5} \pmod{2},$$

where $\overline{x}_j$ denotes $1 - x_j$. Indeed, the nonlinear term is always zero, except at 011011 when it is one, shifting the sequence. We find this a truly beautiful application of mathematics to solve a practical magic problem (see Golomb [6], for further details).

The same problem arises for other universal sequences. Here is a practical example. A Tarot deck consists of 78 cards; there are four suits, each of 14 values for 56 'ordinary' cards, and 22 cards in the 'major arcana'. These are trump cards with colorful names such as 'The Hanged Man'. Tarot cards have been around for over 500 years (see the marvelous history of Stuart Hampshire [7]). They are frequently used for fortune telling, and it is natural to try to invent one of our card tricks using Tarot cards. We use them here as an excuse for discussing available techniques.

One simple approach is to set aside the major arcana, and work with the remaining 56 cards. Now $56 = 8 \cdot 7$. An easy construction is to take the usual de Bruijn sequence 1 0 1 1 1 0 0 0 for eight, and then cut it down to seven as 1 0 1 1 1 0 0 . Taking a product of these two will do the job.

Going back to the full deck of $78 = 6 \cdot 13$. There is a natural universal cycle of length 13 (permutations with ties with window width 3 given in Example 6), as well as one of length 6 (permutations with window width 3). In this case, it is possible to form a product universal cycle since the cycle for permutations with ties does indeed have a block of three repeated symbols. Even easier in this case is to use the fact that the two cycle lengths 13 and 6 are relatively prime. However, a general theory is lacking on how to do this when a sufficiently long block of repeated symbols does not occur in either sequence in the product. To crystallize things, we state the situation as an open problem.

Research Problem. Let $x_1, x_2, \ldots, x_R$ be a universal cycle with window width k. For $k \le j \le R$, is it always possible to find a subsequence of length j which is also a universal cycle with window width k?

4.2 Lifting/Lumping

Lifting involves resizing a universal cycle based on a small alphabet with a larger alphabet. Lumping involves the opposite. Both are well illustrated with universal cycles for permutations. First, consider lifting. In Section 2, we took the product of the permutation cycle 1 3 2 1 3 4 with the binary cycle 1 0 1 1 1 0 0 0. Both have window width $k = 3$. The product construction yields a sequence of 48 pairs (shown in Section 2) with top row 1 3 2 1 3 4 repeated eight times, and bottom row a slightly scrambled version of 1 0 1 1 1 0 0 0 repeated six times. The next problem is to assign card values to these pairs. This was easy for the binary part, using Hearts and Diamonds for 1 (Red), and Clubs and Spades for 0 (Black). This is a primitive lifting. The lifting problem is harder for values. We discard Kings and think of the other card values as $1, 2, 3, \ldots, 12$. The first step was to lift the sequence 1 3 2 1 3 4 (on an alphabet with four symbols) to six distinct symbols: 1 4 3 2 5 6. In fact, we can prove that the following lifting procedure always works: Suppose we have a sequence of digits so that a window of width k gives a distinct relative order as it is run along. Take the highest digit (it may be repeated several times—just choose one) and replace it with $k!$. Take the next highest digit (not counting the $k!$ factorial just created) and replace it by $k! - 1$, and so on. Thus, working right-to-left in 1 3 2 1 3 4 with $k = 3$, we get successively 1 3 2 1 3 6, 1 3 2 1 5 6, 1 4 2 1 5 6, 1 4 3 1 5 6, and finally, 1 4 3 2 5 6. If we had replaced equal digits working left-to-right, the result would have been 2 5 3 1 4 6. Both final sequences have successive groups of three spanning all possible relative orders.

Now consider two adjacent copies 1 4 3 2 5 6 1 4 3 2 5 6. Each 'one' can be assigned to one of $\{1, 2\}$, each 'two' to one of $\{3, 4\}$, and so on, with each 'six' assigned to one of $\{11, 12\}$. Choosing the lower possibility first gives:

$$\begin{array}{cccccccccccc} 1 & 4 & 3 & 2 & 5 & 6 & 1 & 4 & 3 & 2 & 5 & 6 \\ 1 & 7 & 5 & 3 & 9 & 11 & 2 & 8 & 6 & 4 & 10 & 12 \end{array}$$

This pattern is repeated four times and then the suits assigned as explained above. We should point out that consecutive values in $\{1, 2\}, \{3, 4\}$, etc., can be interchanged to make things look more random (as we did in Example 1.).

An example of a lumping problem appears in adapting an arrangement of the numbers $1, 2, 3, \ldots, k!$ with the property that the relative order of each k-tuple is distinct into an arrangement of values in the alphabet $\{1, 2, 3, \ldots, k+1\}$ into a sequence with the same property. For example, when $k = 3$, 1 4 3 2 5 6 can be lumped to 1 3 2 1 3 4. It is easy to see that maximal length permutation sequences cannot be lumped to the alphabet $\{1, 2, 3, \ldots, k\}$. The best that has been proved is $\{1, 2, 3, \ldots, 3k/2\}$ (see [8, 9]). It is conjectured that it is always possible with $\{1, 2, 3, \ldots, k + 1\}$.

Lifting and lumping problems arise all over the subject (see [1] for more examples). We would love to see some theory developed for this problem.

4.3 Coding and Neat Generation

We have not dealt with one aspect of the applications herein. Given the audience's information, how does the performer know what the cards are? We have treated this at some length in our book on mathematics and magic tricks. However, the performer may have the order of the deck available, coupled to the possible patterns. This availability may be through memory (mnemonics), an assistant, or a hidden list. In our popular talks, we often just say "The performer has the information written on his sleeve."

As an indication of the methods presently available, we record a novel approach due to our student Gier Helleloid. It allows a neat decoding for any de Bruijn sequence.

Example 7. Coding a binary de Bruijn cycle. Begin with a fixed de Bruijn cycle of total length m and window width k. We need not have $m = 2^k$. The problem is to assign card values so that the binary color pattern codes the card values in a simple way. Helleloid proposes using a simple *standard* order of the m cards and then use the binary pattern (as a binary number) to determine which card in the standard order goes next.

This is most easily explained by example. Consider the binary de Bruijn cycle 0 0 0 1 1 1 0 1 with $m = 8$ and $k = 3$. Form the standard order of an eight-card deck:

position	0	1	2	3	4	5	6	7
card	AC	$2C$	AS	$2S$	AD	$2D$	AH	$2H$

Here the positions have been labeled (from left to right) $0, 1, 2, 3, 4, 5, 6, 7$ and AC stands for the Ace of Clubs, and so on. Helleloid's rule says to rearrange the standard order as:

$$AC \quad 2C \quad 2S \quad 2H \quad AH \quad 2D \quad AS \quad AD$$

Thus, the first window 0 0 0 of our de Bruijn sequence says to use card in position 0 of the standard order (AC). The next window 0 0 1 says to use the card in position 1 of the standard order ($2C$) next. The next window 0 1 1 says to use the card in position 3 of the standard order ($2S$), next, and so on. The scheme works provided that the standard list has all the Black cards first and all the Red cards last.

For performance, you must be able to easily determine which card is at position j on the standard list. Thus, if the pattern $1\,0\,1$ shows when all with a Red card are asked to stand, the performer translates $1\,0\,1 = 5$, and on the standard list, card 5 is $2D$. This is possible (and even easy) provided the standard list is simple, e.g., for $m = 32$, $k = 5$, we could use $1-8$ of Clubs, $1-8$ of Spades, $1-8$ of Diamonds, $1-8$ of Hearts. To continue beyond the first card, a de Bruijn sequence which can easily be 'run forward' is essential. The shift register sequences discussed in our references are one simple solution. In this case, the next binary digit is a linear combination of the last few. While we know how to do this for de Bruijn sequences, we do not know of analogous procedures for any of our other constructions. Again, we feel it must be possible. There is a fair amount of worthwhile research to be done here.

Appendix: Proof of main theorems and somewhat more.

In this Appendix, we give a proof of Theorem 1 (both windows of equal width) and Theorem 2 (windows of possibly distinct widths). These theorems involve universal *cycles* (going around the corner). They also involve a restriction — one of the cycles must have repeated symbols for all of a window width.

Our proof proceeds by constructing a completely general product (with no restriction on repeated symbols) of two **sequences** (not going around the corner). This is Theorem 3, stated below. Theorems 1 and 2 follow as corollaries.

To state Theorem 3, we need some simple notation. Let

$$\overline{x} = x_1 x_2 \ldots x_R, \quad \overline{y} = y_1 y_2 \ldots y_S, \quad R = rd, \quad S = sd$$

with d being the greatest common divisor of R and S. Thus, r and s have no common divisor (greater than 1). The symbols x_i, y_j are treated as distinct variables. In the corollaries, they may be set to convenient values (e.g., zero or one).

Construction. Construct a two-line array with the top row drawn from the x_i and the second row drawn from the y_j. Both rows will contain RS symbols.

Top Row: Repeat $x_1 x_2 \dots x_R$ a total of S times.

Second Row: Form Y^- by repeating $y_1 y_2 \dots y_s$ a total of r times, and then deleting the final occurrence of y_s. Thus, Y^- has length $rs - 1$. Then, form a sequence of length RS by repeating Y^- a total of d times and adding a total of d repetitions of the symbol y_s at the end.

Example Suppose $\overline{x} = x_1\, x_2$, $\overline{y} = y_1\, y_2\, y_3\, y_4$.

Then $R = 2$, $S = 4$, $d = 2$, $r = 1$, $s = 2$. The construction gives an array of total length 8:

$$\begin{array}{cccccccc} x_1 & x_2 & x_1 & x_2 & x_1 & x_2 & x_1 & x_2 \\ y_1 & y_2 & y_3 & y_1 & y_2 & y_3 & y_4 & y_4 \end{array}$$

Note that each x_1 occurs with each of y_1, y_2, y_3, y_4 exactly once, and this is true for x_2 as well. Theorem 3 says this happens in general.

Theorem 3. Let $\overline{x} = x_1\, x_2 \dots x_R$, $\overline{y} = y_1\, y_2 \dots y_S$, be strings of distinct symbols. Then the construction above produces a two-line array of length RS where each pair $\begin{matrix} x_u \\ y_v \end{matrix}$, $1 \leq u \leq R$, $1 \leq v \leq S$, appears exactly once.

Proof. To check all details, we introduce notation for the blocks of x-symbols in the top row and for the blocks of y-symbols in the second row. Define

$$X = \overbrace{\overline{x}\,\overline{x} \dots \overline{x}}^{s}, \quad Y = \overbrace{\overline{y}\,\overline{y} \dots \overline{y}}^{r}, \quad Y^- = \overbrace{\overline{y}\,\overline{y} \dots \overline{y}}^{r-1} y_1 y_2 \dots y_{s-1}.$$

Thus, X has length rsd as does Y, while Y^- has length $rsd - 1$.

Next, define

$$X_i = X, \quad Y_i^- = Y^-, 1 \leq i \leq d, \quad Z = \overbrace{y_s y_s \dots y_s}^{d}.$$

Finally, the array defined by the construction is

$$\begin{array}{c} X_1\, X_2\, \dots\, X_{d-3}\, X_{d-2}\, X_{d-1}\, X_d \\ Y_1^- \quad Y_2^- \quad \dots\, Y_{d-2}^- \quad Y_{d-1}^- \quad Z. \end{array}$$

Note that each row contains RS symbols. We show that each pair $\begin{array}{c} x_u \\ y_v \end{array}$, $1 \leq u \leq R$, $1 \leq v \leq S$, occurs exactly once. There are two cases.

Case 1: $v \neq sd$.

The indices of the x_u which are paired with y_v in Y_1^- are $u = v, v + sd, v + 2sd, \ldots, v + isd, \ldots, v + (r-1)sd$ where here, and in what follows, we assume index addition is done modulo rd, and instead of 0, we use rd. In Y_2, y_v is paired with x_u for $u = v-1, v-1+sd, \ldots, v-1+isd, \ldots, v-1+(r-1)sd$. In general, in Y_j, y_v is paired with x_u for $u = v - j + 1 + isd$, $0 \leq i \leq r-1$, $1 \leq j \leq d$. We need to show that all these rd values $v - j + 1 + isd$ are distinct modulo rd.

Suppose $v - j + 1 + isd \equiv v - j' + 1 + i'sd \pmod{dr}$, $\quad 0 \leq i, i' \leq r-1$, $1 \leq j, j' \leq d$. Thus, $j' - j + (i - i')sd \equiv 0 \pmod{rd}$. This implies that $j' - j \equiv 0 \pmod{d}$ since $\gcd(r, s) = 1$, which in turn implies that $j = j'$. From this we now conclude that $(i - i')sd \equiv 0 \pmod{rd}$. Consequently, we have $(i - i')s \equiv 0 \pmod{r}$ which implies that $i = i'$. Hence, all the rd indices are distinct, and so, y_v is paired with every possible x_u exactly once, when $v \neq sd$.

Case 2: $v = sd$.

In Y_1^-, y_{sd} is paired with x_u for $u = sd, 2sd, \ldots, (r-1)sd$. In general, in Y_j^-, y_{sd} is paired with x_u for $u = isd - j + 1$, $1 \leq i \leq r-1$, $1 \leq j \leq d$. Also, at the end of the sequence, y_{sd} is paired with the last d symbols of the top row of the array, namely, x_u for $u = dr - d + 1, dr - d + 2, \ldots, dr - 1, dr$.

If $isd - j + 1 \equiv i'sd - j' + 1 \pmod{rd}$ then $j' - j + (i - i')sd \equiv 0 \pmod{rd}$. As before, this implies that $j = j'$ and $i = i'$, so that all these $(r-1)d$ indices are distinct.

Now suppose that $isd - j + 1 \equiv dr - m \pmod{rd}$, $0 \leq m \leq d - 1$. Thus, $isd - j + 1 \equiv -m \pmod{rd}$ from which it follows that $j - 1 \equiv m \pmod{d}$, and finally, that $j = m + 1$. Hence, $isd \equiv 0 \pmod{dr}$, which implies that $i \equiv 0 \pmod{r}$, a contradiction.

Consequently, y_{sd} is paired with every possible x_u exactly once. This completes Case 2 and the theorem is proved. □

Since Theorem 2 is more general than Theorem 1, we need only prove Theorem 2.

Corollary. (Proof of Theorem 2**).**

Take $\overline{x}$ to be an arbitrary universal cycle. It need not have maximal length. Take $\overline{y}$ to be a universal cycle of window length k. We assume that $\overline{y}$ has a block of n repeated symbols which we take to be 0 for notational simplicity. These appear as the last k symbols of $\overline{y}$. Proceed with the construction as above. What has to be checked is that:

(i) When $y_{sd} = 0$ is removed from the end of Y_i to form Y_i^-, then as the window moves across the boundary between Y_i^- and Y_{i+1}^- in $\ldots Y_i^- Y_{i+1}^- \ldots$ we only lose one copy of the block $\overbrace{000\ldots0}^{k}$.

(ii) Since by our construction, $y_{sd} = 0$, then $Z = \overbrace{000\ldots0}^{d}$. Thus, the second row of the array ends with $\overbrace{0000\ldots00}^{k-1+d}$. Since $y_1 \neq 0$ (otherwise $\overline{y}$ would have two blocks equal to $\overbrace{000\ldots0}^{k}$), then as our window of width k goes around the corner in $\ldots Y_{d-1}^- Y_d^- Z Y_1^- \ldots$, we pick up exactly d extra copies of the block $\overbrace{000\ldots0}^{k}$.

Therefore, our construction preserves all necessary occurrences of the required n-tuples in the product. This completes the product construction of the universal cycles $\overline{x}$ and $\overline{y}$, and the proof of Theorem 2 is complete. □

Acknowledgements. Our work on de Bruijn sequences started with card tricks invented with Ronald Wohl. Martin Gardner encouraged us to write these up. These results were presented as a talk at the first **Gathering for Gardner** (Atlanta, 1993). We thank Geir Helleloid for letting use his nice de Bruijn coding in Section 4.3, Hal Fredericksen and Al Hales for comments incorporated in the present version, and Steve Butler for carefully reading the final manuscript.

References

[1] Fan Chung, Persi Diaconis, and Ron Graham, Universal cycles for combinatorial structures, *Discrete Math.*, **110** (1992), 43–59.

[2] Persi Diaconis and Ron Graham, **From Magic to Mathematics–and Back**, Chapters 2, 3 and 4 (to appear).

[3] Persi Diaconis and Ron Graham, (unpublished manuscript).

[4] Hal Fredricksen, A survey of full-length nonlinear shift register cycle algorithms, *SIAM Review* **24** (1982), 195–212.

[5] Martin Gardner **Fractal Music, Hypercards, and more** ..., W. H. Freeman and Company, New York, (1992), x+327 pp., Chap. 2.

[6] Solomon Golomb, **Linear Shift Register Sequences**, Aegean Park Press, Calif., revised edition (1982), Chap. 7.5.

[7] Stuart Hampshire, **The Game of Tarot**, Duckworth Press, London (1980).

[8] Glenn Hurlbert, **On universal cycles for k-subsets of an n-set**, *SIAM J. Discrete Math.* **7** (1994), no. 4, 598–604.

[9] Glenn Hurlbert and Garth Isaac, Equivalence class universal cycles for permutations, *Discrete Math.* **149** (1996), 123–129.

[10] Glenn Hurlbert (personal communication).

[11] Brad Jackson, Universal cycles of k-subsets and k-permutations, *Discrete Math.* **117** (1993), no. 1-3, 141–150.

[12] Brad Jackson, (personal communication).

[13] Don Knuth, **The Art of Computer Programming**, vol. 4, Fascicle 2, Chap. 7.2.1.1, (2005).

[14] Don Knuth, **The Art of Computer Programming**, vol. 4, Fascicle 3, Chap. 7.2.1.5, (2005).

[15] Sherman K. Stein, **Mathematics, The Man Made Universe**, W. H. Freeman, San Francisco, 3rd edition (1976), Chap. 8.