

An inductive approach to constructing universal cycles on the k -subsets of $[n]$

Yevgeniy Rudoy

Johns Hopkins University

Submitted: Oct 28, 2012; Accepted: Apr 16, 2013; Published: Apr 24, 2013

Abstract

In this paper, we introduce a method of constructing universal cycles on sets by taking “sums” and “products” of smaller cycles. We demonstrate this new approach by proving that if there exist universal cycles on the 4-subsets of $[18]$ and the 4-subsets of $[26]$, then for any integer $n \geq 18$ equivalent to 2 (mod 8), there exists a universal cycle on the 4-subsets of $[n]$.

1 Introduction

Consider the binary sequence 00011101. If we regard this sequence as a cycle, each of the 8 binary triples appears exactly once as a block of consecutive symbols in our sequence. In 1946, de Bruijn [1] showed that for any n and k , there exists an n -ary sequence in which each n -ary k -tuple appears exactly once. Such sequences are now known as *de Bruijn cycles*.

In 1992, Chung, Diaconis, and Graham [2] explored various generalizations of de Bruijn cycles, which they called *universal cycles* or *ucycles*. One such generalization was to universal cycles on $\binom{[n]}{k}$ ¹: n -ary sequences in which each block of k consecutive symbols consists of k different symbols, and any set of k symbols chosen from $[n] = \{0, 1, \dots, n-1\}$ is represented exactly once as a set of k consecutive symbols in the sequence.

Chung, Diaconis, and Graham [2] proved that for universal cycles on $\binom{[n]}{k}$ to exist, it is necessary for k to divide $\binom{n-1}{k-1}$, a result reproduced below:

Lemma 1.1 (Chung, Diaconis, and Graham): $k \mid \binom{n-1}{k-1}$ is a necessary condition for the existence of a universal cycle on $\binom{[n]}{k}$.

¹Here, $\binom{[n]}{k}$ denotes the set of all k -element subsets of $[n] = \{0, 1, \dots, n-1\}$

Proof. Let C be a universal cycle on $\binom{[n]}{k}$, and let s be any symbol in $[n]$. For each occurrence of s in C , there will be exactly k different blocks of size k which contain that occurrence of s . Since no block can contain multiple occurrences of s , the total number of blocks containing s must be k times the number of occurrences of s . As there is exactly one such block for each set of k symbols in $[n]$ containing s , k must divide $\binom{n-1}{k-1}$. \square

Chung, Diaconis, and Graham also conjectured that for any k , provided that n was sufficiently large, this necessary condition was also sufficient. In other words,

Conjecture (Chung, Diaconis, and Graham): Ucycles exist for $\binom{[n]}{k}$ provided that k divides $\binom{n-1}{k-1}$ and $n \geq n_0(k)$.

It is easy to show that this conjecture holds when $k \in \{1, 2\}$.

In 1993, Jackson [5] showed that for all $n \geq 8$ not divisible by 3, there exist ucycles on $\binom{[n]}{3}$, completing the $k = 3$ case. The same paper also proved that for odd $n \geq 9$, there exist ucycles on $\binom{[n]}{4}$. Since $\binom{n-1}{3}$ is divisible by 4 if and only if n is odd or $n \equiv 2 \pmod{8}$, this leaves only the $n \equiv 2 \pmod{8}$ case unresolved for $k = 4$.

In 1994, Hurlbert [3] unified Jackson's results and gave a partial solution for $k = 6$ with the following theorem:

Theorem 1.2 (Hurlbert): For $k \in \{3, 4, 6\}$ and sufficiently large n relatively prime to k , there exist ucycles on $\binom{[n]}{k}$.

In addition to the published results above, Jackson claims to have an unpublished result completing the $k = 4$ and proving the $k = 5$ case.

In this paper, we provide a new method of constructing universal cycles on k -subsets of $[n]$. Instead of finding a ucycle directly, we build the ucycle up from smaller cycles. In particular, we demonstrate a method for taking "sums" and "products" of cycles. Although these methods have significant limitations, they give us a powerful new tool for finding universal cycles on sets. In fact, an application of these new techniques allows us to prove the following results:

Main Theorem: If a and b are positive multiples of 8 such that neither $a + 1$ nor $b + 1$ are divisible by 3, then if there exist universal cycles on $\binom{[a+2]}{4}$ and $\binom{[b+2]}{4}$, there must exist universal cycles on $\binom{[a+b+2]}{4}$.

Corollary to Main Theorem: As long as we can find universal cycles on $\binom{[18]}{4}$ and $\binom{[26]}{4}$, we can find universal cycles on 4-subsets on $\binom{[n]}{4}$ for any $n \equiv 2 \pmod{8}$ satisfying $n \geq 18$.

2 Definitions

General

NOTE: IN THIS PAPER, \cup AND “UNION” OF TWO MULTISSETS A AND B WILL BE USED TO DENOTE THE MULTISSET WHICH CONSISTS OF COMBINING THE ELEMENTS WITHOUT REMOVING ANY DUPLICATES. FOR EXAMPLE, WE WOULD SAY

$$\{a, a, b\} \cup \{a, b, c\} = \{a, a, a, b, b, c\}.$$

WE WILL NOT BE USING THE STANDARD SET UNION IN THIS PAPER.

Let $[n] = \{0, 1, \dots, n-1\}$ and $\binom{[n]}{k}$ denote the set of all k -element subsets of $[n]$. Note that this may differ from some conventional definitions of $[n] = \{1, 2, \dots, n\}$.

Define a **k-string** to be a string of length k , and a **k-multiset** to be a multiset of cardinality k .

Denote the cardinality of a multiset A as $|A|$ and the length of a string S as $|S|$.

Define the powerset of a set A , denoted $P(A)$, to be the set of subsets of A . Furthermore, define $P_k(A) = \{M \in P(A) : |M| = k\}$ to be the set of all k -element subsets of A .

If M and N are both multisets of multisets, define their product, $M \times N$, to be the multiset consisting of all the unions of elements of M with elements of N . In other words, $M \times N = \{A \cup B : A \in M, B \in N\}$. For example, if $M = \{\{a, b\}, \{c\}\}$ and $N = \{\{x\}, \{y, z\}\}$, then

$$M \times N = \{\{a, b, x\}, \{a, b, y, z\}, \{c, x\}, \{c, y, z\}\}.$$

If S and T are both strings, let the concatenation of S with T , written $S \cdot T$, be the string consisting of the characters of S followed by the characters of T .

Denote the multiset of k -substrings of S as $\text{SUB}^k(S)$. For example, if $S = abcabcd$, and $k = 3$, we would have $\text{SUB}^k(S) = \{abc, bca, cab, abc, bcd\}$.

If S is a string, let $\Gamma(S)$ denote the multiset of characters in S . If M is a multiset of strings, then let $\Gamma(M)$ denote $\{\Gamma(S) : S \in M\}$. For example, $\Gamma(\text{cycle}) = \{c, c, e, l, y\}$ and $\Gamma(\{\text{and}, \text{text}\}) = \{a, d, e, n, t, t, x\}$.

Cycles

Let a **length z cycle** be a string of length z .

If C is a cycle, let C_x denote the $(x+1)^{\text{th}}$ symbol in C , up to modulo $|C|$. Note that the first symbol of C is C_0 and not C_1 .

If C is a cycle, let C_x^k denote the k -string $C_x C_{x+1} \cdots C_{x+k-2} C_{x+k-1}$.

If C is a cycle, let the **k-range** of C be the multiset $\{C_x^k : 0 \leq x \leq |C| - 1\}$. We will use $R^k(C)$ to denote the k -range of C . For example,

$$R^2(inoh) = \{in, no, oh, hi\}$$

and

$$R^3(abcdabc) = \{abc, bcd, cda, dab, abc, bca, cab\}.$$

Remark: Equivalently, the k -range of C is

$$R^k(C) = \text{SUB}^k(C_0C_1 \cdots C_{|C|+k-3}C_{|C|+k-2}) = \text{SUB}^k(C \cdot C_0^{k-1}).$$

This can be thought of as the multiset of the $|C|$ different length- k substrings of C if we allow “looping over” from the end of C to the beginning of C .

If \mathcal{A} is a set of symbols, we say that C is a **universal cycle** or a **ucycle** on $P_k(\mathcal{A})$ if $\Gamma(R^k(C)) = P_k(\mathcal{A})$. In other words, if C is a universal cycle on $P_k(\mathcal{A})$, then every string in the k -range of C consists of k different symbols in \mathcal{A} , the set of these k symbols is different for each element of C 's k -range, and for any k symbols in \mathcal{A} , there is some element of the k -range of C which consists of these k symbols.

Since $P_k([n]) = \binom{n}{k}$, this new definition agrees with the earlier definition of a universal cycle on $\binom{n}{k}$.

Rotations

We say that a **rotation** of a cycle C is any cycle of the form $C_xC_{x+1} \cdots C_{x+|C|-1}$. In other words, a rotation of C is any cycle which could be obtained from C by repeatedly moving a symbol from the beginning of C to the end of C . For example, the rotations of “ $abc bc$ ” are “ $abc bc$ ”, “ $bc bca$ ”, “ $bc cab$ ”, “ $bc abc$ ”, and “ $cab cb$ ”.

Two simple but important facts follow from this definition. First, rotating a cycle does not change the k -range of the cycle for any k . Second, if S is in the k -range of C , there exists some rotation C' of C such that $S = C'_0C'_1 \cdots C'_{k-1}$; in other words, if S is in C k -range, we can always rotate C so that it starts with S .

3 Cycle Addition

In this section, we present a method for taking the k -sum (\oplus^k) of two cycles to get a new cycle. This operation requires the addends to have a common string of length at least $k - 1$, and has several useful properties which we prove in Theorem 3.2 and its corollary.

Construction

Let S be a $(k - 1)$ -string, and let C and D be cycles containing S . If C' and D' are rotations of C and D which both start with S , we say that $C' \cdot D'$ is a **k-sum** of C and D . Note that S here is arbitrary; all we require is that the first $k - 1$ symbols of C' and D' match.

If there is at least one cycle which is the k -sum of C and D , we will use $C \oplus^k D$ to denote some (arbitrary) k -sum of C and D .

Example

For example, let $C = "abc"$ and $D = "bcdab"$. In this case the 3-sums of C and D are $abc \cdot abcd = abcbbcd$ and $bca \cdot bcdab = bcabcdab$.

Properties

Remark: If C and D have intersecting $(k - 1)$ -ranges, then there is at least one k -sum of C and D .

Lemma 3.1: If E is a k -sum of C and D , then E is a $(k - 1)$ -sum of C and D .

Proof. Since E is a k -sum of C and D , we can write $E = C' \cdot D'$, where C' and D' are rotations of C and D starting with the same $k - 1$ characters. Since C' and D' start with the same $k - 1$ characters, they must also start with the same $k - 2$ characters, so $C' \cdot D' = E$ is also a $(k - 1)$ -sum of C and D . \square

Theorem 3.2: If E is a k -sum of C and D , then the k -range of E is the disjoint-union of the k -ranges of C and D . Formally,

$$R^k(C \oplus^k D) = R^k(C) \cup R^k(D).$$

Proof. Since E is a k -sum of C and D , we can write $E = C' \cdot D'$, where C' and D' are rotations of C and D starting with the same $k - 1$ characters. Let us call the $(k - 1)$ -string of those first characters S .

$$\begin{aligned} R^k(C) &= R^k(C') = \text{SUB}^k(C' \cdot S), \text{ and} \\ R^k(D) &= R^k(D') = \text{SUB}^k(D' \cdot S). \end{aligned}$$

Thus,

$$R^k(C) \cup R^k(D) = \text{SUB}^k(C' \cdot S) \cup \text{SUB}^k(D' \cdot S).$$

But since the last $k - 1$ characters of $\text{SUB}^k(C' \cdot S)$ are the same as the first $k - 1$ characters of $D' \cdot S$,

$$\text{SUB}^k(C' \cdot S) \cup \text{SUB}^k(D' \cdot S) = \text{SUB}^k(C' \cdot D' \cdot S) = \text{SUB}^k(E \cdot S) = R^k(E).$$

□

A simple example of this theorem can be seen for $C = "abc"$, $D = "bcde"$, and $k = 3$. Here, a 3-sum of C and D is $bca \cdot bcde = bcabcde$, and

$$\begin{aligned} R^3(bcabcde) &= \{bca, cab, abc, bcd, cde, deb, dec\} \\ &= \{bca, cab, abc\} \cup \{bcd, cde, deb, dec\} \\ &= \{abc, bca, cab\} \cup \{bcd, cde, deb, dec\} = R^3(C) \cup R^3(D). \end{aligned}$$

Corollary 3.2.1: If E is a k -sum of C and D , then the $(k - 1)$ -range of E is the disjoint-union of the $(k - 1)$ -ranges of C and D .

Proof. By Lemma 2, If E is a k -sum of C and D , it is also a $(k - 1)$ -sum of C and D . Thus, a straightforward application of Theorem 3.2 tells us that $R^{k-1}(E) = R^{k-1}(C) \cup R^{k-1}(D)$. □

Cycle Summation

Sometimes, we will want to take k -sums of more than 2 elements. This leads us to define a generalization over cycle addition which we will call cycle summation. If \mathcal{C} is a set of cycles, we will say that it is **k-summable** if there exists a valid order in which we can add up all the elements of \mathcal{C} . If \mathcal{C} is k -summable, we will furthermore define a **k-summation** of \mathcal{C} , denoted $\bigoplus^k \mathcal{C}$, to any k -sum of the elements of \mathcal{C} taken in some valid order.

Since $R^{k-1}(C \oplus^k D) = R^{k-1}(C) \cup R^{k-1}(D)$, some $C \oplus^k (D \oplus^k E)$ exists if and only if some $C \oplus^k D$ or some $C \oplus^k E$ exists. Thus, \mathcal{C} is k -summable if and only if for any $C, D \in \mathcal{C}$ there exists a set of cycles C_0, C_1, \dots, C_n in \mathcal{C} such that $C = C_0$, $D = C_n$, and for any $i \in [n - 1]$, some $C_i \oplus^k C_{i+1}$ exists.

Remark: We can extend the results of Theorem 3.2 and Corollary 3.2.1 to k -summations. In other words, for any set of cycles \mathcal{C} ,

$$R^k\left(\bigoplus^k \mathcal{C}\right) = \bigcup_{C \in \mathcal{C}} R^k(C) \text{ and}$$

$$R^{k-1}\left(\bigoplus^k \mathcal{C}\right) = \bigcup_{C \in \mathcal{C}} R^{k-1}(C).$$

4 Cycle Multiplication

In the previous section, we saw that if C and D were cycles satisfying certain simple conditions, we could find a cycle $C \oplus^k D$ such that $R^k(C) \cup R^k(D) = R^k(C \oplus^k D)$. It would be desirable to have an analogous result where we could find a cycle E such that $\Gamma(R^t(C)) \times \Gamma(R^u(D)) = \Gamma(R^{t+u}(E))$. Unfortunately, such a cycle is sometimes impossible to find.² Instead, we will show a slightly weaker result: as long as $|C|$ and $|D|$ are both multiples of $t + u$, there is a set of cycles \mathcal{C} such that

$$\Gamma(R^t(C)) \times \Gamma(R^u(D)) = \bigcup_{E \in \mathcal{C}} \Gamma(R^{t+u}(E)).$$

The elements of \mathcal{C} in this result are exactly the WEAVEs that we examine throughout this section.

Construction

Fix two positive integers t and u , and let $k = t + u$. Furthermore, let C and D be cycles such that both $|C|$ and $|D|$ are multiples of k . Then, for any integers c and d , we will define $\text{WEAVE}_{c,d}(C^t, D^u)$ to be the cycle

$$C_c^t \cdot D_d^u \cdot C_{c+t}^t \cdot D_{d+u}^u \cdots C_{c+(r-1)t}^t \cdot D_{d+(r-1)u}^u$$

where $r = \frac{\text{lcm}(|C|u, |D|t)}{tu}$.

Remark: Since k is a factor of both $|C|$ and $|D|$, $k \cdot \text{lcm}(t, u) = \text{lcm}(ku, kt)$ is a factor of $\text{lcm}(|C|u, |D|t)$. But $k = t + u$ is a multiple of $\text{gcd}(t, u)$, so $tu = \text{gcd}(t, u) \cdot \text{lcm}(t, u)$ divides $\text{lcm}(|C|u, |D|t)$. Thus, r is in fact an integer.

Notice that we obtain $\text{WEAVE}_{c,d}(C^t, D^u)$ by “interweaving” C and D : we take t characters from C , then u characters from D , then t characters from C , then u characters from D , and so on. We continue this process, possibly looping over the cycles multiple times, until we simultaneously return to the place we started in both C and D . Since $r = \frac{\text{lcm}(|C|u, |D|t)}{tu}$ is the first value for which both $\frac{rt}{|C|}$ and $\frac{ru}{|D|}$ are integers, this happens after we have used rt characters from C and ru characters from D .

Example

For example, let $t = 3, u = 2, C = 12345$, and $D = abcde$. Then,

$$\text{WEAVE}_{0,0}(C^3, D^2) = 123 \cdot ab \cdot 451 \cdot cd \cdot 234 \cdot ea \cdot 512 \cdot bc \cdot 345 \cdot de.$$

²A simple example of this occurs when $t = u = 1, C = aaa$, and $D = b$. Then, $\Gamma(R^t(C)) \times \Gamma(R^u(D))$ will be $\{\{a, b\}, \{a, b\}, \{a, b\}\}$, which cannot be the 2-range of any cycle.

Properties

NOTE: THROUGHOUT THIS SECTION, WE WILL LET n BE ANY INTEGER, m BE ANY INTEGER SATISFYING $0 \leq m < k$, AND W BE $\text{WEAVE}_{c,d}(C^t, D^u)$.

Remark: $|W| = rt + ru = rk$.

Remark: $W_{nk}^k = C_{c+nt}^t \cdot D_{d+nu}^u$; that is, the length- k substring of W starting at index nk is exactly the concatenation of the length- t substring of C starting at index $c + nt$ with the length- u substring of D starting at index $d + nu$. Note that this holds for all integers n , including those greater than r .

Remark: We can derive an explicit form for the symbol found at a given index of W :

$$W_{nk+m} = \begin{cases} C_{c+nt+m} & 0 \leq m < t \\ D_{d+nu+(m-t)} & t \leq m < k. \end{cases}$$

This allows us to also find an explicit form for the k -substring of W starting from a certain index:

$$W_{nk+m}^k = \begin{cases} C_{c+nt+m}^{t-m} \cdot D_{d+nu}^u \cdot C_{c+(n+1)t}^m & 0 \leq m < t \\ D_{d+nu+(m-t)}^{u-(m-t)} \cdot C_{c+(n+1)t}^t \cdot D_{d+(n+1)u}^{(m-t)} & t \leq m < k. \end{cases}$$

Although this form is not particularly elegant, this result allows us to derive a much more manageable formulation for $\Gamma(W_{nk+m}^k)$ which will be fundamental to our proof of the Product Theorem.

Lemma 4.1:

$$\Gamma((\text{WEAVE}_{c,d}(C^t, D^u))_{nk+m}^k) = \begin{cases} \Gamma(C_{c+nt+m}^t) \cup \Gamma(D_{d+nu}^u) & 0 \leq m < t \\ \Gamma(C_{c+(n+1)t}^t) \cup \Gamma(D_{d+nu+(m-t)}^u) & t \leq m < k. \end{cases}$$

Proof. In the notation of this section, $(\text{WEAVE}_{c,d}(C^t, D^u))_{nk+m}^k = W_{nk+m}^k$, and we can use the result above to compute

$$\begin{aligned}
\Gamma(W_{nk+m}^k) &= \begin{cases} \Gamma\left(C_{c+nt+m}^{t-m} \cdot D_{d+nu}^u \cdot C_{c+(n+1)t}^m\right) & 0 \leq m < t \\ \Gamma\left(D_{d+nu+(m-t)}^{u-(m-t)} \cdot C_{c+(n+1)t}^t \cdot D_{d+(n+1)u}^{(m-t)}\right) & t \leq m < k \end{cases} \\
&= \begin{cases} \Gamma\left(C_{c+nt+m}^t \cdot D_{d+nu}^u\right) & 0 \leq m < t \\ \Gamma\left(D_{d+nu+(m-t)}^u \cdot C_{c+(n+1)t}^t\right) & t \leq m < k \end{cases} \\
&= \begin{cases} \Gamma(C_{c+nt+m}^t) \cup \Gamma(D_{d+nu}^u) & 0 \leq m < t \\ \Gamma(C_{c+(n+1)t}^t) \cup \Gamma(D_{d+nu+(m-t)}^u) & t \leq m < k. \end{cases}
\end{aligned}$$

□

The Product Theorem

We would like to prove

Product Theorem: Let C and D be any cycles for which $|C|$ and $|D|$ are both multiples of $t + u$. Then, there exists a value s such that

$$\Gamma(R^t(C)) \times \Gamma(R^u(D)) = \bigcup_{a=0}^{s-1} \Gamma(R^k(\text{WEAVE}_{a,-a}(C^t, D^u))).$$

We will start by defining two integer functions:

$$F(nk + m) = \begin{cases} nt + m & 0 \leq m < t \\ (n + 1)t & t \leq m < k \end{cases}$$

and

$$G(nk + m) = \begin{cases} nu & 0 \leq m < t \\ nu + (m - t) & t \leq m < k. \end{cases}$$

This allows us to write the result from Lemma 4.1 in a simpler form:

$$\Gamma\left(\left(\text{WEAVE}_{c,d}(C^t, D^u)\right)_{nk+m}^k\right) = \Gamma(C_{c+F(nk+m)}^t) \cup \Gamma(D_{d+G(nk+m)}^u),$$

Equivalently, if we substitute i for $nk + m$,

$$\Gamma\left(\left(\text{WEAVE}_{c,d}(C^t, D^u)\right)_i^k\right) = \Gamma(C_{c+F(i)}^t) \cup \Gamma(D_{d+G(i)}^u),$$

If we let H be the set $\{(F(i), G(i)) : 0 \leq i < rk\}$, it follows that

$$\begin{aligned} \Gamma\left(R^k(\text{WEAVE}_{c,d}(C^t, D^u))\right) &= \left\{ \Gamma(C_{c+F(i)}^t) \cup \Gamma(D_{d+G(i)}^u) : 0 \leq i < rk \right\} \\ &= \left\{ \Gamma(C_{f+c}^t) \cup \Gamma(D_{g+d}^u) : (f, g) \in H \right\}. \end{aligned}$$

To proceed beyond this point we will first need to prove some properties of H .

Remark: $F(i+k) = F(i) + t$ and $G(i+k) = G(i) + u$.

Lemma 4.2: $F(i) + G(i) = i$.

Proof. If we write $i = nk + m$,

$$\begin{aligned} F(i) + G(i) &= F(nk + m) + G(nk + m) \\ &= \begin{cases} (nt + m) + (nu) & 0 \leq m < t \\ ((n+1)t) + (nu + (m-t)) & t \leq m < k \end{cases} \\ &= \begin{cases} nt + m + nu & 0 \leq m < t \\ nt + t + nu + m - t & t \leq m < k \end{cases} \\ &= n(t + u) + m \\ &= i. \end{aligned}$$

□

Throughout this subsection, we will say that two ordered pairs of integers are **similar** (\sim) if their first coordinates are equivalent modulo $|C|$ and their second coordinates are equivalent modulo $|D|$. In other words, $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1 \equiv x_2 \pmod{|C|}$ and $y_1 \equiv y_2 \pmod{|D|}$.

Remark: If $(x_1, y_1) \sim (x_2, y_2)$, then $C_{x_1}^t = C_{x_2}^t$, $D_{y_1}^u = D_{y_2}^u$, and consequently,

$$\Gamma(C_{x_1}^t) \cup \Gamma(D_{y_1}^u) = \Gamma(C_{x_2}^t) \cup \Gamma(D_{y_2}^u).$$

Lemma 4.3: If i and j are integers, we will have $(F(i), G(i)) \sim (F(j), G(j))$ if and only if $j - i$ is a multiple of rk .

Proof. (\Leftarrow): Let $j - i = ark$ for some integer a . Since rt is a multiple of $|C|$ and ru is a multiple of $|D|$,

$$\begin{aligned} F(j) &= F(i + ark) = F(i) + art \equiv F(i) \pmod{|C|} \\ G(j) &= G(i + ark) = G(i) + aru \equiv G(i) \pmod{|D|}. \end{aligned}$$

(\Rightarrow): Let us assume $(F(i), G(i)) \sim (F(j), G(j))$. Since $|C|$ and $|D|$ are both multiples of k , $F(i) \equiv F(j) \pmod{k}$ and $G(i) \equiv G(j) \pmod{k}$, so Lemma 4.2 tells us that

$$i = F(i) + G(i) \equiv F(j) + G(j) = j \pmod{k}.$$

Thus, we can write $j = i + nk$ for some integer n . But $F(i + nk) = F(i) + nt$ and $G(i + nk) = G(i) + nu$, so n must satisfy both $nt \equiv 0 \pmod{|C|}$ and $nu \equiv 0 \pmod{|D|}$. The only such values of n are multiples of $\frac{\text{lcm}(|C|u, |D|t)}{tu} = r$, so $j - i = nk$ is divisible by rk . \square

Lemma 4.4: For any i , exactly one $(f, g) \in H$ satisfies $(f, g) \sim (F(i), G(i))$.

Proof. For any i , there is exactly one value $j \in [rk]$ satisfying $j \equiv i \pmod{rk}$. By Lemma 4.3, j must be the only value in $[rk]$ satisfying

$$(F(j), G(j)) \sim (F(i), G(i)),$$

so $(f, g) = (F(j), G(j))$ is the only element of H satisfying $(f, g) \sim (F(i), G(i))$. \square

Let us define s to be the smallest positive integer for which there exist (f_1, g_1) and (f_2, g_2) in H satisfying $(f_2, g_2) \sim (f_1 + s, g_1 - s)$.³

Lemma 4.5: If (f_1, g_1) and (f_2, g_2) are different elements of H and a and b are integers such that $(f_1 + a, g_1 - a) \sim (f_2 + b, g_2 - b)$, then we must have $|a - b| \geq s$.

Proof. By Lemma 4.4, it is not the case that $(f_1, g_1) \sim (f_2, g_2)$, so our condition that $(f_1 + a, g_1 - a) \sim (f_2 + b, g_2 - b)$ implies $a \neq b$. Without loss of generality, let us assume that $a > b$.

$$\begin{aligned} (f_2 + b, g_2 - b) &\sim (f_1 + a, g_1 - a), \text{ so} \\ (f_2, g_2) &\sim (f_1 + (a - b), g_1 - (a - b)). \end{aligned}$$

Since $(a - b)$ is a positive integer, by definition $s \leq (a - b)$. \square

Lemma 4.6: For any i and any x , there must exist a j satisfying

$$(F(j), G(j)) \sim (F(i) + xs, G(i) - xs).$$

Proof. From the definition of s , we know there must exist some i^* and j^* which satisfy $(F(j^*), G(j^*)) \sim (F(i^*) + s, G(i^*) - s)$. By Lemma 4.2,

$$\begin{aligned} i^* - j^* &= (F(i^*) + G(i^*)) - (F(j^*) + G(j^*)) \\ &= (F(i^*) - F(j^*)) + (G(i^*) - G(j^*)) \\ &\equiv (s) + (-s) \pmod{k}. \end{aligned}$$

Therefore, $i^* - j^*$ is a multiple of k , so we can write $j^* = i^* + nk$, which allows us to compute

$$\begin{aligned} (F(i^*) + nt, G(i^*) + nu) &= (F(j^*), G(j^*)) \sim (F(i^*) + s, G(i^*) - s), \text{ so} \\ (nt, nu) &\sim (s, -s). \end{aligned}$$

³We know such an s must exist because we can let $(f_1, g_1) = (f_2, g_2) = (F(0), G(0))$ and pick s to be a multiple of both $|C|$ and $|D|$.

Let x and i be given, and let $j = i + xnk$. Then,

$$\begin{aligned}(F(j), G(j)) &= (F(i + xnk), G(i + xnk)) \\ &= (F(i) + xnt, G(i) + xnu) \\ &\sim (F(i) + xs, G(i) - xs).\end{aligned}$$

□

Corollary 4.6.1: For any a , $\text{WEAVE}_{a,-a}(C^t, D^u)$ and $\text{WEAVE}_{a+s,-a-s}(C^t, D^u)$ are rotations of each other.

Recall that we have defined s to be the smallest positive integer for which there exist (f_1, g_1) and (f_2, g_2) in H satisfying $(f_2, g_2) \sim (f_1 + s, g_1 - s)$, where

$$H = \{(F(i), G(i)) : 0 \leq i < rk\},$$

where F and G given by

$$\begin{aligned}F(nk + m) &= \begin{cases} nt + m & 0 \leq m < t \\ (n + 1)t & t \leq m < k \end{cases} \\ G(nk + m) &= \begin{cases} nu & 0 \leq m < t \\ nu + (m - t) & t \leq m < k. \end{cases}\end{aligned}$$

Proof. As we saw in the proof of Lemma 4.6, there exists an n satisfying $(nt, nu) \sim (s, -s)$. Thus, for all x and y ,

$$\begin{aligned}F(x) + a + s &\equiv F(x) + a + nt = F(x + nk) + a \pmod{|C|} \\ G(y) - a - s &\equiv G(y) - a + nu = G(y + nk) - a \pmod{|D|},\end{aligned}$$

so for any i ,

$$(\text{WEAVE}_{a+s,-a-s}(C^t, D^u))_i = (\text{WEAVE}_{a,-a}(C^t, D^u))_{i+nk}.$$

□

Theorem 4.7: For any x and y , there is a unique $(f, g) \in H$ and a unique $a \in [s]$ satisfying $(f + a, g - a) \sim (x, y)$.

Proof. By Lemma 4.5, for any a and b in $[s]$, there cannot be two different elements $(f_1, g_1), (f_2, g_2) \in H$ satisfying $(f_1 + a, g_1 - a) \sim (f_2 + b, g_2 - b)$. In addition, if $a, b \in [s]$ are distinct, $(f + a, g + a) \not\sim (f + b, g + b)$. Thus, if some $a \in [s]$ and $(f, g) \in H$ satisfy the conditions of this theorem, they do so uniquely.

Let $i = x + y$, and let $\mu = G(i) - y$. By Lemma 4.2 $F(i) + G(i) = i$, so

$$F(i) + \mu = F(i) + G(i) - y = i - y = x.$$

Thus, $(F(i) + \mu, G(i) - \mu) \sim (x, y)$.

Let a be the value satisfying $a \in [s]$ and $a \equiv \mu \pmod{s}$. By Lemma 4.6, there exists some j for which $(F(j), G(j)) \sim (F(i) + (\mu - a), G(i) - (\mu - a))$. Then,

$$(F(j) + a, G(j) - a) \sim (F(i) + \mu, G(i) - \mu) \sim (x, y).$$

By Lemma 4.4, there exists $(f, g) \in H$ satisfying $(f, g) \sim (F(j), G(j))$, so $(f + a, g - a) \sim (x, y)$. □

Let H^* denote the set of ordered pairs $\{(f + a, g - a) : (f, g) \in H, a \in [s]\}$, and let J denote the set of ordered pairs $\{(x, y) : x \in [|C|], y \in [|D|]\}$.

Corollary 4.7.1: There is a bijection between H^* and J which maps ordered pairs to similar ordered pairs.

Proof. Let $B : H^* \rightarrow J$ be a map which takes any ordered pair in H^* to the element of J which it is similar to. By Theorem 4.7, for any $(x, y) \in J$, there is exactly one element $(f + a, g - a) \in H^*$ such that $B((f + a, g - a)) = (x, y)$, so B must be a bijection. □

We can finally prove the Product Theorem.

Product Theorem: Let C and D be any cycles for which $|C|$ and $|D|$ are both multiples of $k = t + u$.

Let s be the smallest positive integer for which there exist (f_1, g_1) and (f_2, g_2) in H satisfying $(f_2, g_2) \sim (f_1 + s, g_1 - s)$, where

$$H = \{(F(i), G(i)) : 0 \leq i < rk\},$$

where F and G given by

$$F(nk + m) = \begin{cases} nt + m & 0 \leq m < t \\ (n + 1)t & t \leq m < k \end{cases}$$

$$G(nk + m) = \begin{cases} nu & 0 \leq m < t \\ nu + (m - t) & t \leq m < k. \end{cases}$$

Then,

$$\Gamma(R^t(C)) \times \Gamma(R^u(D)) = \bigcup_{a=0}^{s-1} \Gamma(R^{t+u}(\text{WEAVE}_{a,-a}(C^t, D^u))).$$

Proof. We know from the discussion preceding Lemma 4.2 that

$$\Gamma(R^k(\text{WEAVE}_{c,d}(C^t, D^u))) = \left\{ \Gamma(C_{f+c}^t) \cup \Gamma(D_{g+d}^u) : (f, g) \in H \right\}.$$

It follows that

$$\bigcup_{a=0}^{s-1} \Gamma(R^{t+u}(\text{WEAVE}_{a,-a}(C^t, D^u))) = \left\{ \Gamma(C_f^t) \cup \Gamma(D_g^u) : (f, g) \in H^* \right\}.$$

If $(f, g) \sim (x, y)$ then $\Gamma(C_f^t) \cup \Gamma(D_g^u) = \Gamma(C_x^t) \cup \Gamma(D_y^u)$, so by Corollary 4.7.1,

$$\begin{aligned} \left\{ \Gamma(C_f^t) \cup \Gamma(D_g^u) : (f, g) \in H^* \right\} &= \left\{ \Gamma(C_x^t) \cup \Gamma(D_y^u) : (x, y) \in J \right\} \\ &= \left\{ \Gamma(C_x^t) : x \in [|C|] \right\} \times \left\{ \Gamma(D_y^u) : y \in [|D|] \right\} \\ &= \Gamma(R^t(C)) \times \Gamma(R^u(D)). \end{aligned}$$

□

Remark: An application of the Product Theorem shows that

$$|\Gamma(R^t(C)) \times \Gamma(R^u(D))| = \left| \bigcup_{a=0}^{s-1} \Gamma(R^{t+u}(\text{WEAVE}_{a,-a}(C^t, D^u))) \right|,$$

so

$$|C| \cdot |D| = s \cdot |\text{WEAVE}_{a,-a}(C^t, D^u)| = srk = sk \frac{\text{lcm}(|C|u, |D|t)}{tu}.$$

Therefore, we can explicitly compute

$$s = \frac{\text{gcd}(|C|u, |D|t)}{k}.$$

5 Benign Cycles

The Product Theorem show that we can construct a class of cycles

$$\mathcal{C} = \{ \text{WEAVE}_{a,-a}(C^t, D^u) : a \in [s] \}$$

with the property that

$$\bigcup_{E \in \mathcal{C}} \Gamma(R^k(E)) = \Gamma(R^t(C)) \times \Gamma(R^u(D)).$$

However, this is still of little use to us as long as $|\mathcal{C}|$ is large. In this section, we will introduce a method which will allow us to drastically reduce the cardinality of $|\mathcal{C}|$ when the cycle $|C|$ is $(t, t+u)$ -benign. This will leave us with sufficiently few cycles so that we can eventually use cycle addition to construct our universal cycle.

Definition

We say that a cycle C is **(t,k)-benign** if for some Δ relatively prime to $|C|$ and some i , $C_i^{t-1} = C_{i+k\Delta}^{t-1}$. If C is also a universal cycle on S , we would say that C is a (t,k) -benign universal cycle on S .

Examples

For example, the cycle $C = abcdaeed$ is (3,4)-benign since $C_3^2 = da = C_7^2$ and $\frac{7-3}{4} = 1$ is an integer relatively prime to $|C| = 8$.

Application

As usual, let $k = t + u$.

Lemma 5.1: If C and D are cycles with lengths divisible by k and C satisfies $C_i^{t-1} = C_{i+k\Delta}^{t-1}$, then for any a , we can find a k -sum

$$\text{WEAVE}_{a,-a}(C^t, D^u) \oplus^k \text{WEAVE}_{a+u\Delta, -a-u\Delta}(C^t, D^u).$$

Proof. Let \bar{C} denote the rotation of C forward by $k\Delta$ spaces, so \bar{C} satisfies $\bar{C}_x = C_{x+k\Delta}$ for all x . Notice that $\bar{C}_i^{t-1} = C_{i+k\Delta}^{t-1} = C_i^{t-1}$.

For some j , $(\text{WEAVE}_{c,d}(C^t, D^u))_j^{k-1}$ consists of C_i^{t-1} interspersed in some way with u characters from D . But that means $(\text{WEAVE}_{c,d}(\bar{C}^t, D^u))_j^{k-1}$ will consist of \bar{C}_i^{t-1} interspersed in the same way with the same u characters from D . Since $\bar{C}_i^{t-1} = C_i^{t-1}$,

$$(\text{WEAVE}_{c,d}(\bar{C}^t, D^u))_j^{k-1} = (\text{WEAVE}_{c,d}(C^t, D^u))_j^{k-1}.$$

We know from section 4 that

$$\begin{aligned} (\text{WEAVE}_{c,d}(C^t, D^u))_{nk+m} &= \begin{cases} C_{c+nt+m} & 0 \leq m < t \\ D_{d+nu+(m-t)} & t \leq m < k \end{cases}, \text{ so} \\ (\text{WEAVE}_{c+u\Delta, d-u\Delta}(C^t, D^u))_{nk+m} &= \begin{cases} C_{c+u\Delta+nt+m} & 0 \leq m < t \\ D_{d-u\Delta+nu+(m-t)} & t \leq m < k \end{cases} \\ &= \begin{cases} \bar{C}_{c+(n-\Delta)t+m} & 0 \leq m < t \\ D_{d+(n-\Delta)u+(m-t)} & t \leq m < k \end{cases} \\ &= (\text{WEAVE}_{c,d}(\bar{C}^t, D^u))_{(n-\Delta)k+m}. \end{aligned}$$

Therefore, we can conclude that

$$\begin{aligned} (\text{WEAVE}_{c+u\Delta, d-u\Delta}(C^t, D^u))_{j+k\Delta}^{k-1} &= (\text{WEAVE}_{c,d}(\overline{C}^t, D^u))_j^{k-1} \\ &= (\text{WEAVE}_{c,d}(C^t, D^u))_j^{k-1}, \end{aligned}$$

so for any c and d , we can find a k -sum

$$\text{WEAVE}_{c,d}(C^t, D^u) \oplus^k \text{WEAVE}_{c+u\Delta, d-u\Delta}(C^t, D^u).$$

By setting $d = -c$, this reduces to the result we were looking for. \square

Lemma 5.2: If C and D are cycles with lengths divisible by k , C is a (t, k) -benign cycle, and $s = \frac{\gcd(|C|u, |D|t)}{k}$, then there exists a partition of

$$\mathcal{C} = \{\text{WEAVE}_{a,-a}(C^t, D^u) : a \in [s]\}$$

into $\gcd(u, s)$ multisets \mathcal{C}_i such that

1. For any $a \in [s]$, if $i \in [\gcd(u, s)]$ and a is equivalent to i modulo $\gcd(u, s)$, then $\text{WEAVE}_{a,-a}(C^t, D^u) \in \mathcal{C}_i$, and
2. Each \mathcal{C}_i is k -summable.

Proof. Let W_a denote $\text{WEAVE}_{a,-a}(C^t, D^u)$.

Since C is a (t, k) -benign cycle, we can find Δ relatively prime to $|C|$ and i such that $C_i^{t-1} = C_{i+k\Delta}^{t-1}$. By Lemma 5.1, for any a there exists a k -sum $W_a \oplus^k W_{a+u\Delta}$. By Corollary 4.6.1, W_a and W_{a+s} are equivalent up to rotation for any a , so if a and b satisfy the relation $b \equiv a + u\Delta \pmod{s}$, we can take the k sum of W_a and W_b .

Since Δ is relatively prime to $|C|$ and s divides $|C|$, Δ must be relatively prime to s . Thus, there must exist a value $\overline{\Delta}$ satisfying $\Delta\overline{\Delta} \equiv 1 \pmod{s}$.

Let \mathcal{C}_i be the multiset of W_a for which $a - i$ is a multiple of $\gcd(u, s)$. Notice that $\{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{\gcd(u, s)}\}$ is a partition of \mathcal{C} , and $W_a \in \mathcal{C}_i$ for any a equivalent to i modulo $\gcd(u, s)$.

For any $W_a, W_b \in \mathcal{C}_i$, a is equivalent to b modulo $\gcd(u, s)$. Since any multiple of $\gcd(u, s)$ can be written as an integer linear combination of u and s , and $b - a$ is a multiple of $\gcd(u, s)$, there must exist integers y, z such that $b - a = yu + zs$. Therefore,

$$b = a + yu + zs \equiv a + yu \equiv a + (y\overline{\Delta})(u\Delta) \pmod{s}.$$

If we let $a_x = a + xu\Delta$, we get $a_0 = a$, $a_{y\overline{\Delta}} = b$, and $a_{i+1} \equiv a_i + u\Delta \pmod{s}$. By the last condition, we can take a k -sum of W_{a_i} and $W_{a_{i+1}} = W_{(a_i+u\Delta)}$, so by the criterion established in Section 3, \mathcal{C}_i must be k -summable. \square

Corollary 5.2.1: If C and D are cycles having lengths divisible by k and C is $(t, t+u)$ -benign, then there exist $x \leq u$ multisets \mathcal{C}_i such that

1. For any a , if $i \in [x]$ and $i \equiv a \pmod{x}$, $\text{WEAVE}_{a,-a}(C^t, D^u) \in \mathcal{C}_i$,
2. Each \mathcal{C}_i is k -summable, and
3. If we let \mathcal{C} denote $\bigcup_{i=0}^{x-1} \mathcal{C}_i$,

$$\Gamma(R^t(C)) \times \Gamma(R^u(D)) = \bigcup_{E \in \mathcal{C}} \Gamma(R^{t+u}(E)).$$

Proof. Let $s = \frac{\gcd(|C|u, |D|t)}{k}$ and $x = \gcd(u, s)$ (note that $\gcd(u, s) \leq u$, so x satisfies $x \leq u$). By the product theorem, $\mathcal{C} = \{\text{WEAVE}_{a,-a}(C^t, D^u) : a \in [s]\}$ satisfies

$$\Gamma(R^t(C)) \times \Gamma(R^u(D)) = \bigcup_{E \in \mathcal{C}} \Gamma(R^{t+u}(E)),$$

so this corollary follows directly from Lemma 5.2. □

Existence of Important Cases

Remark: Since $C_i^0 = C_j^0$ for any i, j , any cycle is $(1, k)$ -benign for arbitrary k .

Lemma 5.3: For any $k > 3$ and any odd $n \geq 2k - 1$, there exists a $(2, k)$ -benign universal cycle on $\binom{[n]}{2}$.

Proof. For any w , let $D_w(x)$ be the cycle which has length $\frac{n}{\gcd(w, n)}$ whose symbols are given by $(D_w(x))_i \equiv x + iw \pmod{n}$, $(D_w(x))_i \in [n]$.⁴ Less formally, $D_w(x)$ is the unique cycle which starts at x , has symbols taken from $[n]$, obeys the condition that each symbol must be w greater (modulo n) than the last, and goes until it loops back to x for the first time.

Note that all of the $\frac{n}{\gcd(w, n)}$ symbols of $D_w(x)$ are unique, and are actually the symbols in $[n]$ which are equivalent to x modulo $\gcd(w, n)$. Thus, the 2-range of $D_w(x)$ will be the set of strings ij for which i and j are both in $[n]$, i is equivalent to x modulo $\gcd(w, n)$, and $j \equiv i + w \pmod{n}$.

Now, let $\mathcal{D}_w = \{D_w(x) : 0 \leq x < \gcd(w, n)\}$. We can see that

$$\bigcup_{D \in \mathcal{D}_w} R^2(D) = \left\{ ij : i \in [n], j \in [n], j \equiv i + w \pmod{n} \right\}.$$

⁴Note that our definition of $(D_w(x))_i \equiv x + iw \pmod{n}$ is periodic, with a period exactly equal to the length of $D_w(x)$.

If we also let $\mathcal{D} = \bigcup_{w=1}^{\frac{n-1}{2}} \mathcal{D}_w$, then

$$\bigcup_{D \in \mathcal{D}} \Gamma(R^2(D)) = \left\{ \{i, j\} : i \in [n], j \in [n], i \neq j \right\} = P_2([n]).$$

Let $\mathcal{D}' = \mathcal{D} - \{D_{k-1}(0), D_1(0)\}$. Since $\frac{n-1}{2} \geq k > 3$, and $k \neq 2$, both \mathcal{D} and \mathcal{D}' will contain $D_2(0)$.

Since 2 must be relatively prime to n , $D_2(0)$ must contain every symbol in $[n]$, which means its 1-range must intersect with the 1-range of every element of \mathcal{D}' . Thus, \mathcal{D}' is 2-summable.

Let E denote some such 2-summation with a first symbol of '0'.

Since $D_{n-1}(0)_0^1 = D_{k-1}(0)_0^1 = E_0^1 = 0$, we can take their k -summation $E' = D_{n-1}(0) \cdot D_{k-1}(0) \cdot E$. But

$$\Gamma(R^2(D_{n-1}(0))) = \Gamma(R^2(D_1(0))),$$

so

$$\begin{aligned} \Gamma(R^2(E')) &= \Gamma(R^2(D_{n-1}(0))) \cup \Gamma(R^2(D_{k-1}(0))) \cup \Gamma(R^2(E)) \\ &= \Gamma(R^2(D_1(0))) \cup \Gamma(R^2(D_{k-1}(0))) \cup \Gamma(R^2(E)) \\ &= \Gamma\left(\bigcup_{D \in \mathcal{D}} (R^2(D))\right) \\ &= \left\{ \{i, j\} : i \in [n], j \in [n], i \neq j \right\}. \end{aligned}$$

Thus, E' is a universal cycle on $\left[\begin{smallmatrix} n \\ 2 \end{smallmatrix}\right]$.

$E'_{n-(k-1)} = D_{n-1}(0)_{n-(k-1)} = k-1$ and $E'_{n+1} = D_{k-1}(0)_1 = k-1$. Since

$$n+1 - (n - (k-1)) = k \cdot 1$$

and 1 is relatively prime to $|E'|$, E' must be $(2, k)$ -benign. □

6 Proof of the Main Theorem

In this section, we will finally prove our main theorem:

Main Theorem: If a and b are positive multiples of 8 such that neither $a+1$ nor $b+1$ are divisible by 3, then if there exist universal cycles on $\left[\begin{smallmatrix} a+2 \\ 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} b+2 \\ 4 \end{smallmatrix}\right]$, there must exist universal cycles on $\left[\begin{smallmatrix} a+b+2 \\ 4 \end{smallmatrix}\right]$.

Preliminaries

Lemma 6.1: If C is a universal cycle on $P_k(\mathcal{A})$, $|\mathcal{A}| = |\mathcal{B}|$, S is a $(k + 1)$ -string consisting of $k + 1$ distinct symbols from \mathcal{B} , and x is any integer, then there exist a cycle D such that

1. $D_x^{k+1} = S$
2. D is a universal cycle on $P_k(\mathcal{B})$, and
3. if C is (a, b) -benign, then so is D .

Proof. Since $|\mathcal{A}| = |\mathcal{B}|$, we can find a bijection from \mathcal{A} to \mathcal{B} . Furthermore, for any distinct $a_1, a_2, \dots, a_n \in \mathcal{A}$ and distinct $b_1, b_2, \dots, b_n \in \mathcal{B}$, we can find such a bijection which maps each a_i to b_i .

Since C is universal cycle on $P_k(\mathcal{A})$, C_x^k and C_{x+1}^k must each consist of k different symbols. In addition, since we must have $\Gamma(C_x^k) \neq \Gamma(C_{x+1}^k)$, $C_x \neq C_{x+k}$, so C_x^{k+1} consists of $k + 1$ different characters.

Let f be some bijection from \mathcal{A} to \mathcal{B} which takes C_{x+i} to S_i for every $i \in [k + 1]$, and let $D = f(C)$. Then, for $i \in [k + 1]$, $D_{x+i} = f(C_{x+i}) = S_i$, so $D_x^{k+1} = S$.

In addition,

$$\begin{aligned} R^k(D) &= \{D_x^k : 0 \leq x \leq |D| - 1\} \\ &= \{f(C)_x^k : 0 \leq x \leq |C| - 1\} \\ &= \{f(C_x^k) : 0 \leq x \leq |C| - 1\} \\ &= f(\{C_x^k : 0 \leq x \leq |C| - 1\}) \\ &= f(P_k(\mathcal{A})) \\ &= P_k(\mathcal{B}). \end{aligned}$$

Finally, if C is (a, b) -benign, then $C_i^{a-1} = C_{i+b\Delta}^{a-1}$, so

$$D_i^{a-1} = f(C)_i^{a-1} = f(C_i^{a-1}) = f(C_{i+b\Delta}^{a-1}) = f(C)_{i+b\Delta}^{a-1} = D_{i+b\Delta}^{a-1},$$

which shows that D must also be (a, b) -benign. □

Let a and b be positive integers for which

1. Both a and b are divisible by 8,
2. neither $a + 1$ nor $b + 1$ are divisible by 3, and
3. there exist universal cycles on $\left[\frac{a+2}{4}\right]$ and $\left[\frac{b+2}{4}\right]$.

Remark: $a \geq 16$ and $b \geq 16$.

Let \mathcal{A} and \mathcal{B} be disjoint sets of symbols satisfying $|\mathcal{A}| = a$ and $|\mathcal{B}| = b$. Let α and β be distinct symbols not in $\mathcal{A} \cup \mathcal{B}$.

Let

$$\begin{aligned} M_0 &= P_4(\mathcal{A} \cup \{\alpha, \beta\}) \\ M_1 &= P_3(\mathcal{A} \cup \{\alpha\}) \times P_1(\mathcal{B}) \\ M_2 &= P_2(\mathcal{A} \cup \{\alpha\}) \times P_2(\mathcal{B} \cup \{\beta\}) \\ M_3 &= P_1(\mathcal{A}) \times P_3(\mathcal{B} \cup \{\beta\}) \\ M_4 &= P_4(\mathcal{B} \cup \{\alpha, \beta\}). \end{aligned}$$

Remark:

$$M_0 \cup M_1 \cup M_2 \cup M_3 \cup M_4 = P_4(\mathcal{A} \cup \mathcal{B} \cup \{\alpha, \beta\}).$$

Constructing the Component Cycles

NOTE: THE PROPERTIES OF CYCLES CONSTRUCTED IN THIS SUBSECTION ARE SUMMARIZED IN FIGURE 1.

Since $a + 1$ is odd and greater than $7 = 2 \cdot 4 - 1$, by Lemma 5.3 there exists a $(2, 4)$ -benign universal cycle on $[\frac{a+1}{2}]$. Thus, by Lemma 6.1, we can find a cycle $C(2)$ which is a $(2, 4)$ -benign ucycle on $P_2(\mathcal{A} \cup \{\alpha\})$ satisfying $\alpha \notin \Gamma(C(2)_1^3)$.

By similar reasoning, we can find a ucycle on $P_2(\mathcal{B} \cup \{\beta\})$ satisfying $\beta \notin \Gamma(D(2)_{-2}^3)$.

For any set M , we can obtain a universal cycle on $P_1(M)$ simply by listing the characters of M in any order. Since $C(2)_1^3$ contains only characters from \mathcal{A} , we can find a cycle $C(3)$ which is a universal cycle on $P_1(\mathcal{A})$ satisfying $C(3)_0^3 = C(2)_3 C(2)_1 C(2)_2$.

By similar reasoning, we can find a cycle $D(1)$ which is a universal cycle on $P_1(\mathcal{B})$ satisfying $D(1)_0^3 = D(2)_0 D(2)_{-2} D(2)_{-1}$.

Since $a + 1 \geq 8$ and $a + 1$ is not a multiple of 3, by the results of Jackson [5], there exist universal cycles on $[\frac{a+1}{3}]$. Thus, by Lemma 6.1, we can find a cycle $C(1)$ which is a universal cycle on $P_3(\mathcal{A} \cup \{\alpha\})$ satisfying $C(1)_{-2}^4 = C(2)_0^4$, and therefore also satisfying $C(1)_{-2}^3 = C(2)_0^3$.

By similar reasoning, we can find a cycle $D(3)$ which is a universal cycle on $P_3(\mathcal{B} \cup \{\beta\})$ satisfying $D(3)_{-2}^3 = D(2)_{-1}^3$.

By assumption, there exist universal cycles on $[\frac{a+2}{4}]$ and $[\frac{b+2}{4}]$. Thus, by Lemma 6.1, we can find a cycle $C(0)$ which is a universal cycle on $P_4(\mathcal{A} \cup \{\alpha, \beta\})$ satisfying $C(0)_{-1}^4 = C(1)_{-1}^4$.

By similar reasoning, we can find a cycle $D(4)$ which is a universal cycle on $P_4(\mathcal{B} \cup \{\alpha, \beta\})$ satisfying $D(4)_0^4 = D(3)_{-1}^4$.

Remark: $|C(1)|, |C(2)|, |C(3)|, |D(1)|, |D(2)|$, and $|D(3)|$ are each divisible by 4.

$$C(3)_0^3 = C(2)_3 C(2)_1 C(2)_2, \text{ so} \qquad C(3)_0 = C(2)_3 \qquad (1)$$

$$C(3)_1^3 = C(2)_3 C(2)_1 C(2)_2, \text{ so} \qquad C(3)_1 = C(2)_1 \qquad (2)$$

$$C(3)_2^3 = C(2)_3 C(2)_1 C(2)_2, \text{ so} \qquad C(3)_2 = C(2)_2 \qquad (3)$$

$$C(1)_{-2}^3 = C(2)_0^3, \text{ so} \qquad C(1)_{-2}^2 = C(2)_0^2 \qquad (4)$$

$$C(1)_{-2}^3 = C(2)_0^3, \text{ so} \qquad C(1)_{-1}^2 = C(2)_1^2 \qquad (5)$$

$$C(0)_{-1}^4 = C(1)_{-1}^4, \text{ so} \qquad C(0)_{-1}^3 = C(1)_{-1}^3 \qquad (6)$$

$$C(0)_{-1}^4 = C(1)_{-1}^4, \text{ so} \qquad C(0)_0^3 = C(1)_0^3 \qquad (7)$$

$$D(1)_0^3 = D(2)_0 D(2)_{-2} D(2)_{-1}, \text{ so} \qquad D(1)_0 = D(2)_0 \qquad (8)$$

$$D(1)_0^3 = D(2)_0 D(2)_{-2} D(2)_{-1}, \text{ so} \qquad D(1)_1 = D(2)_{-2} \qquad (9)$$

$$D(1)_0^3 = D(2)_0 D(2)_{-2} D(2)_{-1}, \text{ so} \qquad D(1)_2 = D(2)_{-1} \qquad (10)$$

$$D(3)_{-2}^3 = D(2)_{-1}^3, \text{ so} \qquad D(3)_{-2}^2 = D(2)_{-1}^2 \qquad (11)$$

$$D(3)_{-2}^3 = D(2)_{-1}^3, \text{ so} \qquad D(3)_{-1}^2 = D(2)_0^2 \qquad (12)$$

$$D(4)_0^4 = D(3)_{-1}^4, \text{ so} \qquad D(4)_0^3 = D(3)_{-1}^3 \qquad (13)$$

$$D(4)_0^4 = D(3)_{-1}^4, \text{ so} \qquad D(4)_1^3 = D(3)_0^3 \qquad (14)$$

Figure 1: Summary of what we know by construction

Remark:

$$\begin{aligned} M_0 &= \Gamma (R^4 (C(0))) \\ M_1 &= \Gamma (R^3 (C(1))) \times \Gamma (R^1 (D(1))) \\ M_2 &= \Gamma (R^2 (C(2))) \times \Gamma (R^2 (D(2))) \\ M_3 &= \Gamma (R^1 (C(3))) \times \Gamma (R^3 (D(3))) \\ M_4 &= \Gamma (R^4 (D(4))). \end{aligned}$$

Fitting Everything Together

Let us define

$$\begin{aligned} E_i(1) &= \text{WEAVE}_{i,-i}(D(1)^1, C(1)^3), \\ E_i(2) &= \text{WEAVE}_{i,-i}(C(2)^2, D(2)^2), \\ E_i(3) &= \text{WEAVE}_{i,-i}(C(3)^1, D(3)^3), \\ \mathcal{H}(1) &= \{E_0(1), E_1(1), E_2(1)\}, \\ \mathcal{H}(2) &= \{E_0(2), E_1(2)\}, \text{ and} \\ \mathcal{H}(3) &= \{E_0(3), E_1(3), E_2(3)\}. \end{aligned}$$

Lemma 6.2: $\{C(0), D(4)\} \cup \mathcal{H}(1) \cup \mathcal{H}(2) \cup \mathcal{H}(3)$ is 4-summable.

Proof. First,

$$\begin{aligned} C(0)_{-1}^3 &= C(1)_{-1}^3 = E_1(1)_1^3 && \text{By Fig.1(6)} \\ C(0)_0^3 &= C(1)_0^3 = E_0(1)_1^3 && \text{By Fig.1(7)}. \end{aligned}$$

Thus, $\{C(0), E_0(1), E_1(1)\}$ must be 4-summable.

$$\begin{aligned} E_0(1)_{-2}^3 &= C(1)_{-2}^2 D(1)_0 = C(2)_0^2 D(2)_0 = E_0(2)_0^3 && \text{By Fig.1(4, 8)} \\ E_2(1)_0^3 &= D(1)_2 C(1)_{-2}^2 = D(2)_{-1} C(2)_0^2 = E_0(2)_{-1}^3 && \text{By Fig.1(4, 10),} \end{aligned}$$

so $\{C(0), E_0(2)\} \cup \mathcal{H}(1)$ must be 4-summable.

$$\begin{aligned} E_1(1)_0^3 &= D(1)_1 C(1)_{-1}^2 = D(2)_{-2} C(2)_1^2 = E_1(2)_{-1}^3 && \text{By Fig.1(5, 9)} \\ E_0(3)_{-2}^3 &= D(3)_{-2}^2 C(3)_0 = D(2)_{-1}^2 C(2)_3 = E_1(2)_2^3 && \text{By Fig.1(1, 11)} \\ E_2(3)_0^3 &= C(3)_2 D(3)_{-2}^2 = C(2)_2 D(2)_{-1}^2 = E_1(2)_1^3 && \text{By Fig.1(3, 11)} \\ E_1(3)_0^3 &= C(3)_1 D(3)_{-1}^2 = C(2)_1 D(2)_0^2 = E_0(2)_1^3 && \text{By Fig.1(2, 12),} \end{aligned}$$

so $\{C(0)\} \cup \mathcal{H}(1) \cup \mathcal{H}(2) \cup \mathcal{H}(3)$ must be 4-summable.

Finally,

$$D(4)_1^3 = D(3)_0^3 = E_0(3)_1^3 \quad \text{By Fig.1(14).}$$

Thus, $\{C(0), D(4)\} \cup \mathcal{H}(1) \cup \mathcal{H}(2) \cup \mathcal{H}(3)$ must be 4-summable. \square

Main Theorem: If a and b are positive multiples of 8 such that neither $a + 1$ nor $b + 1$ are divisible by 3, then if there exist universal cycles on $\left[\begin{smallmatrix} a+2 \\ 4 \end{smallmatrix} \right]$ and $\left[\begin{smallmatrix} b+2 \\ 4 \end{smallmatrix} \right]$, there must exist universal cycles on $\left[\begin{smallmatrix} a+b+2 \\ 4 \end{smallmatrix} \right]$.

Proof. $D(1)$ is $(1, 4)$ -benign (trivially), so by Corollary 5.2.1⁵ we can find $x \leq 3$ multisets $\mathcal{C}(1)_i$ such that

⁵Note that in this application of the corollary, $D(1)$ takes on the role of C , and $C(1)$ takes on the role of D , despite the notational mismatch.

1. each $\mathcal{C}(1)_i$ contains an element of $\mathcal{H}(1)$,
2. each element of $\mathcal{H}(1)$ is contained in one of the $\mathcal{C}(1)_i$,
3. each $\mathcal{C}(1)_i$ is 4-summable, and
4. If we let $\mathcal{C}(1) = \bigcup_{i=0}^{x-1} \mathcal{C}(1)_i$,

$$\bigcup_{E \in \mathcal{C}(1)} \Gamma(R^4(E)) = \Gamma(R^1(D(1))) \times \Gamma(R^3(C(1))) = M_1.$$

Since $\{C(0), D(4)\} \cup \mathcal{H}(1) \cup \mathcal{H}(2) \cup \mathcal{H}(3)$ is 4-summable by Lemma 6.2, properties 1, 2, and 3 above imply that $\{C(0), D(4)\} \cup \mathcal{H}(2) \cup \mathcal{H}(3) \cup \mathcal{C}(1)$ is 4-summable.

$C(3)$ is (1, 4)-benign (trivially), so by Corollary 5.2.1 we can find $x \leq 3$ multisets $\mathcal{C}(3)_i$ such that

1. each $\mathcal{C}(3)_i$ contains an element of $\mathcal{H}(3)$,
2. each element of $\mathcal{H}(3)$ is contained in one of the $\mathcal{C}(3)_i$,
3. each $\mathcal{C}(3)_i$ is 4-summable, and
4. If we let $\mathcal{C}(3) = \bigcup_{i=0}^{x-1} \mathcal{C}(3)_i$,

$$\bigcup_{E \in \mathcal{C}(3)} \Gamma(R^4(E)) = \Gamma(R^1(C(3))) \times \Gamma(R^3(D(3))) = M_3.$$

Since $\{C(0), D(4)\} \cup \mathcal{H}(2) \cup \mathcal{H}(3) \cup \mathcal{C}(1)$ is 4-summable, properties 1, 2, and 3 above imply that $\{C(0), D(4)\} \cup \mathcal{H}(2) \cup \mathcal{C}(1) \cup \mathcal{C}(3)$ is 4-summable.

$C(2)$ is (2, 4)-benign by construction, so by Corollary 5.2.1 we can find $x \leq 2$ multisets $\mathcal{C}(2)_i$ such that

1. each $\mathcal{C}(2)_i$ contains an element of $\mathcal{H}(2)$,
2. each element of $\mathcal{H}(2)$ is contained in one of the $\mathcal{C}(2)_i$,
3. each $\mathcal{C}(2)_i$ is 4-summable, and
4. If we let $\mathcal{C}(2) = \bigcup_{i=0}^{x-1} \mathcal{C}(2)_i$,

$$\bigcup_{E \in \mathcal{C}(2)} \Gamma(R^4(E)) = \Gamma(R^2(C(2))) \times \Gamma(R^2(D(2))) = M_2.$$

Since $\{C(0)\} \cup \mathcal{H}(2) \cup \mathcal{C}(1) \cup \mathcal{C}(3)$ is 4-summable, properties 1, 2, and 3 above imply that $\{C(0), D(4)\} \cup \mathcal{C}(1) \cup \mathcal{C}(2) \cup \mathcal{C}(3)$ is 4-summable.

Let $\mathcal{C} = \{C(0), D(4)\} \cup \mathcal{C}(1) \cup \mathcal{C}(2) \cup \mathcal{C}(3)$.

$$\bigcup_{E \in \mathcal{C}} \Gamma(R^4(E)) = M_0 \cup M_4 \cup M_1 \cup M_2 \cup M_3 = P_4(\mathcal{A} \cup \mathcal{B} \cup \{\alpha, \beta\}).$$

Since \mathcal{C} is 4-summable, there must exist a cycle X whose 4-range is the union of the 4-ranges of the elements of \mathcal{C} , which means

$$\Gamma(R^4(X)) = P_4(\mathcal{A} \cup \mathcal{B} \cup \{\alpha, \beta\}).$$

Thus, X is a universal cycle on $P_4(\mathcal{A} \cup \mathcal{B} \cup \{\alpha, \beta\})$.

Since $|\mathcal{A} \cup \mathcal{B} \cup \{\alpha, \beta\}| = a + b + 2$, and a universal cycle on $\left[\begin{smallmatrix} a+b+2 \\ 4 \end{smallmatrix} \right]$ exists if and only if a universal cycle on $P_4(\mathcal{A} \cup \mathcal{B} \cup \{\alpha, \beta\})$ exists, there must exist a universal cycle on $\left[\begin{smallmatrix} a+b+2 \\ 4 \end{smallmatrix} \right]$. \square

Corollary to Main Theorem: As long as we can find universal cycles on $\left[\begin{smallmatrix} 18 \\ 4 \end{smallmatrix} \right]$ and $\left[\begin{smallmatrix} 26 \\ 4 \end{smallmatrix} \right]$, we can find universal cycles on 4-subsets on $\left[\begin{smallmatrix} n \\ 4 \end{smallmatrix} \right]$ for any $n = 2 \pmod{8}$ satisfying $n \geq 18$.

Proof. Let us assume that there exist universal cycles on $\left[\begin{smallmatrix} 18 \\ 4 \end{smallmatrix} \right]$ and $\left[\begin{smallmatrix} 26 \\ 4 \end{smallmatrix} \right]$. Since 16 is a multiple of 8 and is not equivalent to 2 (mod 3), by the Main Theorem, there must exist a universal cycle on $\left[\begin{smallmatrix} 16+16+2 \\ 4 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 34 \\ 4 \end{smallmatrix} \right]$. Thus, we know that any $i \in \{2, 3, 4\}$, there exists a universal cycle on $\left[\begin{smallmatrix} 8i+2 \\ 4 \end{smallmatrix} \right]$. From here, we proceed by induction on i .

Let us assume that $x \geq 4$ and for any i satisfying $2 \leq i \leq x$, there exists a universal cycle on $\left[\begin{smallmatrix} 8i+2 \\ 4 \end{smallmatrix} \right]$.

If $x \equiv 2 \pmod{3}$, $8 \cdot (x-2) + 1$ is not divisible by 3. Since $24 + 1$ is not divisible by 3 and there exist universal cycles on $\left[\begin{smallmatrix} 8(x-2)+2 \\ 4 \end{smallmatrix} \right]$ and $\left[\begin{smallmatrix} 24+2 \\ 4 \end{smallmatrix} \right]$, there must exist a universal cycle on $\left[\begin{smallmatrix} 8(x-2)+24+2 \\ 4 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 8(x+1)+2 \\ 4 \end{smallmatrix} \right]$.

If $x \not\equiv 2 \pmod{3}$, $8 \cdot (x-1) + 1$ is not divisible by 3. Since $16 + 1$ is not divisible by 3 and there exist universal cycles on $\left[\begin{smallmatrix} 8(x-1)+2 \\ 4 \end{smallmatrix} \right]$ and $\left[\begin{smallmatrix} 16+2 \\ 4 \end{smallmatrix} \right]$, there must exist a universal cycle on $\left[\begin{smallmatrix} 8(x-1)+16+2 \\ 4 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 8(x+1)+2 \\ 4 \end{smallmatrix} \right]$.

Thus, by induction, for any $i \geq 2$, there exists a universal cycle on $\left[\begin{smallmatrix} 8i+2 \\ 4 \end{smallmatrix} \right]$. \square

7 Future Directions

The $k = 5$ case

In this paper, we have demonstrated several methods of fitting together small cycles to make larger ones. These methods allowed us to prove our Main Theorem, but they are not limited to this application. For example, they could be used to make significant inroads on the $k = 5$ case. In particular, we could show:

Conjecture: For any $i \in \{1, 2, 3, 4\}$, if a and b are sufficiently large multiples of 5 and satisfy certain other divisibility conditions⁶, then if there exist universal cycles on $\left[\frac{a+i}{5}\right]$ and $\left[\frac{b+i}{5}\right]$, there must exist universal cycles on $\left[\frac{a+b+i}{5}\right]$.

This result could be achieved entirely with the tools presented in Sections 2 through 5 by modifying Section 6 to use slightly different component cycles. Unfortunately, the divisibility conditions on a and b would limit $a + b + i$ to even values, so even with the correct base cases, this would only solve the problem of finding universal cycles on $\left[\frac{n}{5}\right]$ for even n . Of course, it is quite possible that other approaches might yield less restricted results.

The $k > 5$ cases

When $k > 5$, our approach runs into a difficulty. Recall that in the proof of the Main Theorem, we used the fact that $C(3)$ and $D(1)$ were $(1, 4)$ -benign and $C(2)$ was $(2, 4)$ -benign. For the $k = 5$ case, we would similarly have two component cycles which were $(1, 5)$ -benign and two which were $(2, 5)$ -benign. But for the $k = 6$ case, this approach would require a component cycle which was $(3, k)$ -benign; a case our construction does not extend to.

To resolve this issue, we would need to prove the existence of $(3, k)$ -benign universal cycles on $\left[\frac{n}{3}\right]$ for various n . To make further inroads on the $k > 7$ cases, we would need to prove the existence of $(4, k)$ -benign universal cycles on $\left[\frac{n}{4}\right]$, and so on. We suspect that this may be possible to do by modifying the existence proofs in [3] or [5] to conform to this benignity condition, which would allow us to apply our methods to higher k .

Generalizing Weaves

In this paper, we describe a method of “multiplying” two cycles. A natural question would be whether it is possible to similarly multiply three or more cycles, and indeed there is. If we have x cycles $C(1), C(2), \dots, C(x)$ such that $|C(i)|$ is a multiple of $k = t(1) + t(2) + \dots + t(x)$ for any i , then we can create a Weave of these cycles by taking $t(1)$ symbols from $C(1)$, $t(2)$ symbols from $C(2)$, $t(3)$ symbols from $C(3)$, and continue in this fashion (returning to $C(1)$ after taking symbols from $C(x)$) until adding the symbols from $C(x)$ returns us to the place we started in each of the $C(i)$. Interestingly enough, the “divisibility by k ” condition is sufficient for the following generalization of the Product Theorem to hold:

⁶These conditions would be the analogues to the Main Theorem’s condition that neither $a + 1$ nor $b + 1$ are divisible by 3, arising partially from the necessity of finding the smaller universal cycles we use, and partially from the fact that we can only weave together cycles whose lengths are multiples of k . The conditions will depend on both i and how we fit the cycles together (namely, what we chose to be the analogues to M_0, M_1, M_2, M_3 and M_4).

Generalized Product Theorem (proof omitted)⁷: Let $C(i)$ for $i \in \{1, 2, \dots, x\}$ be cycles such that $k = t(1) + t(2) + \dots + t(x)$ divides $|C(i)|$ for each i . Then, there is a set A of x -tuples such that

$$\begin{aligned} & \Gamma(R^{t(1)}(C(1))) \times \Gamma(R^{t(2)}(C(2))) \times \dots \times \Gamma(R^{t(x)}(C(x))) \\ &= \bigcup_{(a(1), \dots, a(x)) \in A} \Gamma(R^k(\text{WEAVE}_{a(1), \dots, a(x)}(C(1)^{t(1)}, \dots, C(x)^{t(x)}))). \end{aligned}$$

Although this result was not necessary for the $k = 4$ case, it greatly expands the options we have for expressing a cycle as a sum of products of cycles - some of which may yield additional progress on the Chung, Diaconis, and Graham conjecture.

Universal Cycles on other Combinatorial Families

Although we have focused on the problem of finding universal cycles on k -subsets of n -sets, our methods can also be applied to finding universal cycles on other combinatorial families. For instance, they could be used to finding universal cycles on k -multisets on n -sets, a problem studied by Hurlbert, Johnson, and Zahl in [4]. In fact, the Product Theorem would be applicable to any combinatorial family which consisted of some subset of the k -multisets on an n -set, an example being the k -multisets containing exactly k' distinct symbols.

Acknowledgments

We thank Anant Godbole, whose supervision and support made this work possible. We also thank Sam Hopkins for his thorough reading of this paper, and Bradley Jackson for showing us his work on the subject. This research was supported by NSF Grant 1004624.

8 References

- [1] N.G. de Bruijn, A combinatorial problem, *Nederl. Akad. Wetensch.* **49** (1946), 758-764.
- [2] F.R.K. Chung, P. Diaconis, R.I. Graham, Universal Cycles for Combinatorial Structures, *Discrete Math.* **110** (1992), 43-59.
- [3] G. Hurlbert, On Universal Cycle for k -subsets of an n -set, *SIAM J. Discrete Math.* **7** (1994), 598-604.
- [4] G. Hurlbert, T. Johnson, J. Zahl, On Universal Cycles for Multisets, *Discrete Math.* **309** (2009), 5321-5327
- [5] B. Jackson, Universal Cycles for k -subsets and k -permutations, *Discrete Math.* **117** (1993), 141-150.

⁷A proof of this is quite similar to our proof of the Product Theorem.