Permanents of Circulants: a Transfer Matrix Approach*
(Extended Abstract)

Mordecai J. Golin      Yiu Cho Leung      Yajun Wang

Abstract
Calculating the permanent of a (0,1) matrix is a #P-complete problem but there are some classes of structured matrices for which the permanent is calculable in polynomial time. The most well-known example is the fixed-jump (0,1) circulant matrix which, using algebraic techniques, was shown by Minc to satisfy a constant-coefficient fixed-order recurrence relation.

In this note we show how, by interpreting the problem as calculating the number of cycle-covers in a directed circulant graph, it is straightforward to reprove Minc’s result using combinatorial methods. This is a two step process: the first step is to show that the cycle-covers of directed circulant graphs can be evaluated using a transfer matrix argument. The second is to show that the associated transfer matrices, while very large, actually have much smaller characteristic polynomials than would a-priori be expected.

An important consequence of this new viewpoint is that, in combination with a new recursive decomposition of circulant-graphs, it permits extending Minc’s result to calculating the permanent of the much larger class of circulant matrices with non-fixed (but linear) jumps.

1 Introduction

Definition 1.1. Let $A = (a_{i,j})$ be an $n \times n$ matrix. Let $S_n$ be the set of permutations of the integers $[1, \ldots, n]$. The permanent of $A$ is

$$\text{Perm}(A) = \sum_{\pi \in S_n} \prod_{i=1}^{n} a_{i, \pi(i)} \text{ where } \pi = [\pi(1), \ldots, \pi(n)].$$

If $A$ is a (0,1) matrix, then $A$ can be interpreted as the adjacency matrix of some directed graph $G$ and $\text{Perm}(A)$ is the number of directed cycle-covers in $G$, where a directed cycle-cover is a collection of disjoint cycles that cover all of the vertices in the graph. Alternatively, $A$ can be interpreted as the adjacency matrix of a bipartite graph $G$, in which case $\text{Perm}(A)$ is the number of perfect-matchings in $G$. The permanent is a classic well-studied combinatorial object (see the book and later survey by Minc[13, 16]).

Calculating the permanent of a (0,1) matrix is a #P-Complete problem [19] even when $A$ is restricted to have only 3 non-zero entries per row [8]. The best known algorithm for calculating a general permanent is a straightforward inclusion-exclusion technique due to Ryser [13] running in $\Theta(n2^n)$ time and polynomial space. By allowing super-polynomial space, Bax and Franklin [1] developed a slightly faster (although still exponential) algorithm for the (0,1) case. We point out, in another direction, that just recently, Jerrom, Sinclair and Vigoda [11] developed a fully polynomial approximation scheme for approximating the permanent of nonnegative matrices.

On the other hand, for certain special structured classes of matrices one can exactly calculate the permanent in “polynomial time”. The most studied example of such a class is probably the circulant matrices, which, as discussed in [7], can be thought of as the borderline between the easy and hard cases.

An $n \times n$ circulant matrix $A = (a_{i,j})$ is defined by specifying its first row; the $(i+1)^{th}$ row is a cyclic shift $i$ units to the right of the first row, i.e., $a_{i,j} = a_{1,1+(n+j-i) \text{ mod } n}$. Let $P_n$ denote the $(0,1)$ $n \times n$ matrix with 1s in positions $(i, i+1)$, $i = 1, \ldots, n-1$, and $(n,1)$ and 0s everywhere else. Many of the early papers on this topic express circulant matrices in the form

$$(1.1) \quad A_n = a_1 P_n^{s_1} + a_2 P_n^{s_2} + \cdots + a_k P_n^{s_k}$$

where $0 \leq s_1 < s_2 < \cdots < s_k < n$ and $a_i = a_{1,s_i+1}$.

The first major result on permanents of (0,1) circulants is due to Metropolis, Stein and Stein [12]. Let $k > 0$ be fixed and $A_{n,k} = \sum_{i=0}^{k-1} P_n^{i}$ be the $n \times n$ circulant matrix whose first row is composed of 1s in its first $k$ columns and 0s everywhere else. Then [12] showed that, as a function of $n$, $\text{Perm}(A_{n,k})$ satisfies a fixed order constant-coefficient recurrence relation in $n$.

*Partially supported by HK CERG grants HKUST6162/00E, HKUST6082/01E and HKUST6206/02E. Dept. of Computer Science, Hong Kong U.S.T., Clear Water Bay, Kowloon, Hong Kong. Email addresses are {golin,esco,yalding}@cs.ust.hk.
and therefore, could be calculated in polynomial time in \( n \) (after a superpolynomial “start-up cost” in \( k \) for deriving the recurrence relation).

This result was greatly improved by Minc who showed that it was only a very special case of a general rule. Let \( 0 \leq s_1 < s_2 < \cdots < s_k < n \) be any fixed sequence and set \( A_n = A_n(s_1, \ldots, s_k) = P_{n_1} + P_{n_2} + \cdots + P_{n_k} \). In [14, 15] Minc proved that \( \text{Perm}(A_n) \) always satisfies a constant-coefficient recurrence relation in \( n \) of order \( 2^k - 1 \). Minc’s theorem was proven by manipulating algebraic properties of \( A_n \). Note, that as mentioned by Minc, this result is difficult to apply for large \( s_k \) since, in order to derive the coefficients of the recurrence relation it is first necessary to evaluate \( \text{Perm}(A_n) \) for \( n \leq 2(2^k - 1) \) and, using, Ryser’s algorithm, this requires \( \Omega(2^{2^k}) \) time.

Later Codenotti, Resta and various coauthors improved these results in various ways; e.g. in [2] showing how to evaluate sparse circulant matrices of size \( \leq 200 \); in [4, 5] showing that the permanents of circulants with only three 1s per row can be evaluated in polynomial time; in [6] showing how the permanents of some special sparse circulants can be expressed in terms of determinants and are therefore soluble in polynomial time; in [2] showing that the permanents of dense circulants are hard to calculate and in [7] that even approximating the permanent of an arbitrary circulant modulo a prime \( p \) is “hard” unless \( \mathbf{P} \neq \mathbf{P} \mathbf{P} \).

In this paper we return to the original problem of Minc. Our first main result will be to show that if circulant matrix \( A_n(s_1, \ldots, s_k) \) is interpreted as the adjacency matrix of a directed circulant graph \( C_n \), then counting the number of cycle-covers of \( C_n \) using a transfer matrix approach immediately reproves Minc’s result. As well as reproving Minc’s original result this new technique will then permit us extend the result to a much larger set of circulant graphs as well as address other related problems. To explain, we first need to introduce some notation.

**Definition 1.2.** See Figure 1. Let \( C_{n_1, s_2, \ldots, s_k} \) be the \( n \)-node directed circulant graph with jumps \( S = \{ s_1, s_2, \ldots, s_k \} \). (Note that in this definition we allow negative \( s_i \).) Formally,

\[
C_{n_1, s_2, \ldots, s_k} = (V(n), E_C(n))
\]

where \( V(n) = \{0, 1, \ldots, n - 1\} \) and \( E_C(n) = \{(i, j) : (j - i) \mod n \in S\} \).

Note: we will assume that \( S \) contains at least one non-negative \( s_i \) since if all the \( s_i \) were negative we could multiply them by \(-1\) and get an isomorphic graph. Also, we will often write \( C_n \) as shorthand for \( C_{n_1, s_2, \ldots, s_k} \).

Let \( G = (V, E) \) be a graph, \( T \subseteq E \) and \( v \in V \). Define \( \text{ID}_T(v) \) to be the indegree of \( v \) in graph \((V, T)\) and \( \text{OD}_T(v) \) to be the outdegree of \( v \) in \((V, T)\). \( T \subseteq E \) is a cycle-cover of \( G \) if

\[
\forall v \in V, \quad \text{ID}_T(v) = \text{OD}_T(v) = 1.
\]

**Definition 1.3.** Let \( S = \{s_1, s_2, \ldots, s_k\} \) be given. Set

\[
\mathcal{C}(n) = \{T \subseteq C : T \text{ is a cycle-cover of } C_n\}
\]

and

\[
T(n) = \mathcal{C}(n) \quad \text{No. of cycle-covers of } C_n.
\]

Note that, by the standard correspondence mentioned before, \( A_n(s_1, \ldots, s_k) \) is the adjacency matrix of \( C_{n_1, s_2, \ldots, s_k} \) and \( T(n) = \text{Perm}(A_n(s_1, \ldots, s_k)) \). So, calculating \( T(n) \) is equivalent to calculating permanents of \( A_n(s_1, \ldots, s_k) \).

In [9, 10] the authors of this paper were interested in counting spanning trees and other structures in undirected circulant graphs. The main tool introduced there was a recursive decomposition of such graphs. In Section 2 we describe a related recursive decomposition of directed circulant graphs. Our technique will be to use this decomposition to show that for some constant \( m \) there is a \( m \times 1 \) (column) vector function \( \tilde{T}(n) \) such that

\[
\forall n \geq 2^k, \quad T(n) = \beta \tilde{T}(n) \text{ and } \tilde{T}(n + 1) = A \tilde{T}(n)
\]

(1.2)

where \( \beta \) is a constant to be defined later (but reduces to \( \beta = s_k \) for the Minc formulation described previously), \( A \) is a \( 1 \times m \) constant row-vector and \( A \) is a constant \( m \times m \) matrix. Such an \( A \) is known as a transfer-matrix see, e.g., [18].

Let \( P(x) = \sum_{i=0}^t p_i x^i \) be any polynomial that annihilates \( A \), i.e., \( P(A) = 0 \). Then it is easy to see that \( \forall n \geq 2^k \)

\[
\sum_{i=0}^t p_i T(n+i) = \beta \left( \sum_{i=0}^t p_i A^{n+i-2^k} \right) \tilde{T}(2^k)
\]

\[
= \beta A^{-2^k} \left( \sum_{i=0}^t p_i A^i \right) \tilde{T}(2^k)
\]

\[
= \beta A^{-2^k} 0 \tilde{T}(2^k)
\]

\[
= 0
\]

where \( 0 \) denotes the \( m \times m \) zero matrix and \( 0 \) a scalar; \( \tilde{T}(n) \) thus satisfies the degree-\( t \) constant coefficient recurrence relation \( \tilde{T}(n+t) = \sum_{i=0}^{t-1} -\frac{p_i}{\beta} \tilde{T}(n+i) \) in \( n \). By
the Cayley-Hamilton theorem, the characteristic polynomial of $A$, which has degree $\leq m$, must annihilate $A$, so such a polynomial exists and $T(n)$ satisfies a recurrence relation of at most degree $m$. In our notation, Minc’s theorem is that $T(n)$ satisfies a recurrence relation of degree $2^s - 1$. Unfortunately, in our construction, $m = 2^s$ so the characteristic polynomial does not suffice for our purposes. Our next step will involve showing that even though $A$ is of size $2^{2s} \times 2^{2s}$, there is a much smaller $P$, of degree $2^s - 1$, that annihilates $A$, thus reproving Minc’s theorem. We point out that this degree reduction of the transfer matrix (to the square-root of the original size) is, a-priori, quite unexpected, and does not occur in the undirected-circulant counting problems analyzed in [9, 10].

One interesting consequence of this new derivation is that, unlike in Minc’s proof, to derive the recurrence relation it is no longer necessary to start by spending $\Omega \left(2^{2^s}\right)$ time calculating the first $2^s$ values of $T(n)$ using Ryser’s method. Instead one only has to calculate $A$, $\beta$, the polynomial $P$ and the first $2^s$ values of $T(n)$ which, as we will see later, can all be done in $O(s2^{2s})$ time, reducing the start-up complexity from doubly-exponential in $s$ to singularly exponential.

Another, albeit minor, consequence of this new derivation is that it can also handle non $(0, 1)$ circulants. That is, given any matrix $A_n$ of the form (1), even when the $a_i$ are not restricted to be in $\{0, 1\}$ the technique shows that $\text{Perm}(A_n)$ satisfies a recurrence relation of degree $2^s - 1$. This is only a minor consequence, though, since working through the details of Minc’s original proof is it possible to modify it to get the same result.

A much more important new consequence, and the major motivation for this paper, is the fact that the proof can be extended to evaluate the permanents of non-constant jump circulant matrices, something which has not been addressed before. To explain this, we generalize Definition 1.2 to

**Definition 1.4.** See Figure 2(a). Let $p, s, p_1, p_2, \ldots, p_k$ and $s_1, s_2, \ldots, s_k$ be fixed integral constants with such that $0 \leq p_i < p$. Set $S = \{(p_1 n + s_1, p_2 n + s_2, \ldots, p_k n + s_k)\}$. Denote the $(pn + s)$-node directed circulant graph with jumps $S$ by

\[
C_n = C_{pn+s}^{p_1 n + s_1, p_2 n + s_2, \ldots, p_k n + s_k} = (V(n), E_C(n))
\]

where

\[
V(n) = \{0, 1, \ldots, pn + s - 1\}
\]

and

\[
E_C(n) = \{(i, j) : (j - i) \mod (pn + s) \in S\}.
\]

Note that $A_{pn+s}(p_1 n + s_1, p_2 n + s_2, \ldots, p_k n + s_k)$ is the adjacency matrix of $C_n$ so, counting the cycle-covers in $C_n$ is equivalent to evaluating $\text{Perm}(A_{pn+s}(p_1 n + s_1, p_2 n + s_2, \ldots, p_k n + s_k))$. Our method of counting the cycle covers in $C_n$ will be to derive a new recursive decomposition of $C_n$ (which might be of independent interest) and use it to show that an analogue of (1.2) holds in the non-constant jump case as well; thus $T(n)$ still satisfies a constant-coefficient recurrence relation in $n$. For example, in Table 1, we show the recurrence relation for the number of cycle covers in $C_{3n}^{1, n + 1, 2n}$ and $C_{3n}^{0, n, 2n - 1}$.

In the next section we describe the new recursive decompositions of $C_n$, for both constant and non-constant jumps, upon which our technique is based. In Section 3 we show how this permits easily reproving Minc’s result for non-constant circulants. We then describe the minor modifications that are needed to extend the proof to non-constant circulants.

**Note:** Due to space limitations in this extended abstract only the proof skeleton is given, with many
The main conceptual difficulty with deriving a recurrence relation for $T(C_n)$ is that larger circulant graphs can not be built recursively out of smaller ones. The crucial observation, though, is that, there is another graph, $L_n$, the lattice graph, that can be built recursively, and $C_n$ can then be constructed from $L_n$ through the addition of a constant number of edges\footnote{To put this into context, this is very similar to the definition of Recursive families for undirected graphs \cite{3,17}.}. In \cite{9,10} the authors of this paper developed such a recursive decomposition for undirected circulant graphs as a tool for counting the number of spanning trees in such graphs. In what follows we develop a corresponding decomposition for directed circulants that will permit counting cycle-covers.

We first show this for the restricted case in which $S$, the set of jumps, is constant (independent of $n$), where it is easy to visualize. After deriving the relevant properties we extend the decomposition to the more complicated case in which the set of jumps can depend upon $n$.

**Definition 2.1.** See Figure 1. Let $S = \{s_1, s_2, \ldots, s_k\}$, where the $s_i$ are fixed integers. Define the $n$-node lattice graph with jumps $S$

$$L_n^{s_1,s_2,\ldots,s_k} = (V(n), E_L(n))$$

where

$$E_L(n) = \left\{ (i,j) : j - i \in S \right\}.$$ 

Now set

$$\text{Hook}(n) = E_C(n) - E_L(n)$$

and

$$\text{New}(n) = E_L(n+1) - E_L(n).$$

Note that this implies

$$(2.3) L_{n+1} = L_n \cup \text{New}(n) \quad \text{and} \quad C_n = L_n \cup \text{Hook}(n).$$

The simple but important observation is that, when $n$ is viewed as a label rather than as a number, $\text{Hook}(n)$ and $\text{New}(n)$ are independent of the actual value of $n$.

---

Figure 2: $C_{3n}^{1,n,2n}$, a non-constant jump circulant. Dashed edges are $\text{Hook}(n)$. Solid edges are $L_n$. (a) and (b) are two representations of the graph when $n = 4$. Note the lattice representation in (b). (c) is the case $n = 5$. The bold solid edges on the right are $\text{New}(n)$. The 3 vertices on the right are $V N(n)$. Note that the dashed $\text{Hook}(n)$ edges for both $n = 4,5$ are “independent” of $n$.

<table>
<thead>
<tr>
<th>$C_n^{1,0,1}$</th>
<th>$C_n^{0,1,2}$</th>
<th>$C_{3n}^{1,n+1,2n}$</th>
<th>$C_{3n}^{0,n,2n-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T(n) = 2T(n-1) - T(n-3)$</td>
<td>$T(n) = 5T(n-1) - 5T(n-2) - 5T(n-3) + 6T(n-4)$</td>
<td>$T(n) \sim \phi^n$</td>
<td>$T(n) \sim 3^n$</td>
</tr>
<tr>
<td>initial values 17, 45, 113, 309 for $n = 2,3,4,5$</td>
<td>initial values 17, 45, 113, 309 for $n = 2,3,4,5$</td>
<td>$\phi = (1 + \sqrt{5})/2$</td>
<td>$\phi = (1 + \sqrt{5})/2$</td>
</tr>
</tbody>
</table>

Table 1: The number of cycle-covers $T(n)$ in directed circulant graphs with constant jumps $C_n^{1,0,1}$ and $C_n^{0,1,2}$, and with non-constant jumps $C_{3n}^{1,n+1,2n}$ and $C_{3n}^{0,n,2n-1}$, as derived by the technique in this paper. Note that inside each pair of graphs, the number of cycle covers is the same. This is to be expected, since their adjacency matrices are just linear circular shifts of each other so the permanents of their adjacency matrices are the same.
Lemma 2.1. Set $S^+ = \{s \in S : s \geq 0\}$ and $S^- = \{s \in S : s < 0\}$. Then

\[ \text{Hook}(n) = \left( \bigcup_{s \in S^+} \{(n-j, s-j) : 1 \leq j \leq s\} \right) \]

\[ \cup \left( \bigcup_{s \in S^-} \{(j, n+s+j) : 0 \leq j < |s|\} \right) \]

\[ \text{New}(n) = \left( \bigcup_{s \in S^+} \{(n-s, n)\} \right) \cup \left( \bigcup_{s \in S^-} \{(n, n+s)\} \right) \]

Further set $s^+ = \max_{s \in S^+} s$, and $s^- = \max_{s \in S^-} |s|$ (if $S^- = \emptyset$ set $s^- = 0$).

For later use we define $s = s^+ + s^-$. Now define

\[ L^+(n) = \{0, \ldots, s^+ - 1\}, \]

\[ R^+(n) = \{n - s^+, \ldots, n - 1\}, \]

\[ L^-(n) = \{0, \ldots, s^- - 1\}, \]

\[ R^-(n) = \{n - s^-, \ldots, n - 1\}. \]

Then

\[ \text{Hook}(n) \subseteq \left( R^+(n) \times L^+(n) \right) \cup \left( L^-(n) \times R^-(n) \right) \]

\[ \text{New}(n) \subseteq \left( R^+(n) \times \{n\} \right) \cup \left( \{n\} \times R^-(n) \right) \]

(2.4)

\[ \cup \{(n, n)\} \]

Important Note: In this section and the next we will always assume that $n \geq 2s$ since this will guarantee that $(L^+(n) \cup L^-(n)) \cap (R^+(n) \cup R^-(n)) = \emptyset$. Without this assumption some of our proofs would fail. Also note that the term in $\text{New}(n)$ is only needed when $0 \in S$.

We now extend the above definitions and lemmas to the case of non-constant circulants. This will require a change in the way that we visualize the nodes of $C_n$; until now, as in Figure 1(c), we visualized them as points on a line with the edges in $\text{Hook}(n)$ connecting the left and right endpoints of the line. In the non-constant jump case it will be convenient to visualize them as points on a bounded-height lattice, where $\text{Hook}(n)$ connects the left and right boundaries of the lattice. We start by introducing a new graph:

Definition 2.2. See Figure 2. Let $p, s, p_1, p_2, \ldots, p_k$ and $s_1, s_2, \ldots, s_k$ be given integral constants such that $\forall i, 0 \leq p_i < p$. Set $S = \{p_1n + s_1, p_2n + s_2, \ldots, pkn + s_k\}$. For $u, v$ and integer $n$, set $f(n; u, v) = un + v$. Define

\[ \widehat{C}_n = \left( \widehat{V}(n), \widehat{E}(n) \right) \]

where

\[ \widehat{V}(n) = \{(u, v) : 0 \leq u \leq p - 1, 0 \leq v \leq n - 1\} \]

and $\widehat{E}(n)$ is the set of the union of all edges

\[ ((u_1, v_1), (u_2, v_2)) \]

where the union is taken over all

\[ (u_1, v_1), (u_2, v_2) \in \widehat{V}(n) \]

such that

\[ f(n; u_2, v_2) = f(n; u_1, v_1) \mod (pn + s) \subseteq S. \]

Directly from the definition we see $\widehat{C}_n$ is isomorphic to $C_n = C_{pn + s_1, p_2n + s_2, \ldots, pkn + s_k}$. In particular, cycle-covers of $\widehat{C}_n$ are in 1-1 correspondence with cycle covers of $C_n$ so we can restrict ourselves to counting cycle covers of $\widehat{C}_n$. We now introduce the generalization of Definition 2.1.

Definition 2.3. Let $p, s, p_1, p_2, \ldots, p_k$ and $s_1, s_2, \ldots, s_k$ and $S$ be as in Definition 2.2. Define the $pn + s$-node lattice graph with jumps $S$

\[ L_n = (\widehat{V}(n), \widehat{E}(n)) \]

where $\widehat{E}(n)$ is the set of the union of all edges

\[ ((u_1, v_1), (u_2, v_2)) \]

where the union is taken over all

\[ (u_1, v_1), (u_2, v_2) \in \widehat{V}(n), \]

such that

\[ f(n; u_2, v_2) = f(n; u_1, v_1) = pn + s \mod (pn + s) \]

and

\[ u_2 - u_1 = p_i \mod p. \]

Now set

\[ \text{Hook}(n) = \widehat{E}(n) - \widehat{E}(n) \]

and

\[ \text{New}(n) = \widehat{E}(n + 1) - \widehat{E}(n). \]

Note that this implies

\[ L_{n+1} = L_n \cup \text{New}(n) \]

(2.5)

\[ \widehat{C}_n = L_n \cup \text{Hook}(n). \]

It is now straightforward to derive an analogue of Lemma 2.1 showing that $\text{Hook}(n)$ and $\text{New}(n)$ are independent of the actual value of $n$. Let $NV(n) = V_L(n + 1) - V_L(n)$. $NV(n)$ will be the new vertices in $V_L(n + 1)$. Note that we did not define this for fixed-jump circulant graphs since in the fixed-jump case there is only the one new vertex $V_L(n + 1) - V_L(n) = \{n\}$ and $NV(n)$ would be constant.
Lemma 2.2. Set $S^+ = \{s_i \in S : s_i \geq 0\}$, $S^- = \{s_i \in S : s_i < 0\}$, and $s^+ = \max_{s_i \in S^+} s_i$, $s^- = \max_{s_i \in S^-} |s_i|$. Let $t_1 = s^+ - 1$, $t_2 = s^- - 1$ and $r = \min \{-s, 0\}$. Now let $0 \leq u \leq p - 1$ and define

$$L^+(n) = \{(u, v) : 0 \leq v \leq \max\{t_1, t_1 + s\}\},$$
$$R^+(n) = \{(u, n - 1 - v) : r \leq v \leq \max\{t_1, t_1 - s\}\},$$
$$L^-(n) = \{(u, n - 1 - v) : r \leq v \leq \max\{t_2 + s, t_2 + 2s\}\},$$
$$R^-(n) = \{(u, n - 1 - v) : r \leq v \leq \max\{t_2, t_2 + 2s\}\}.$$

Then

$$\text{Hook}(n) \subseteq (R^+(n) \times L^+(n))$$
$$\cup (L^-(n) \times R^-(n)),$$

(2.6) $$\text{New}(n) \subseteq (R^+(n) \times NV(n))$$
$$\cup (NV(n) \times R^-(n))$$
$$\cup (NV(n) \times NV(n)).$$

3 A New Proof of Minc’s result

Let $CC$ be a cycle-cover of $C_n$. Then, in $T = CC - \text{Hook}(n)$, almost all vertices $v$ except possibly those that have an edge of $\text{Hook}(n)$ hanging off of them, have $\text{ID}_T(v) = \text{OD}_T(v) = 1$. Referring to (2.4) this motivates

Definition 3.1. $T \subseteq E_L(n)$ is a legal cover of $L_n$ if

- $\forall v \in V, \text{ID}_T(v) \leq 1$ and $\text{OD}_T(v) \leq 1$.
- $\forall v \in V - (L^+(n) \cup R^-(n)), \text{ID}_T(v) = 1$.
- $\forall v \in V - (L^-(n) \cup R^+(n)), \text{OD}_T(v) = 1$.

Then, from (2.4) we have

Lemma 3.1.

(a) If $T \subseteq E_C(n)$ is a cycle-cover of $C_n$, then $T - \text{Hook}(n)$ is a legal-cover of $L_n$.

(b) If $T \subseteq E_L(n + 1)$ is a legal-cover of $L_{n+1}$, then $T - \text{New}(n)$ is a legal-cover of $L_n$.

From the definition of legal covers we can classify and partition legal covers by the appropriate in/out degrees of their vertices in $L^+(n)$, $L^-(n)$, $R^+(n)$, $R^-(n)$.

Definition 3.2. A is a binary $r$-tuple if $A = (A(0), A(1), \ldots, A(r - 1))$ where $\forall i, A(i) \in \{0, 1\}$.

Let $P$ be the set of $2s^+$ tuples $(L_+, L_-, R_+, R_-)$ where $L_+, L_-, R_+, R_-$ are, respectively, binary $s^+$, $s^-$, $s^+$, $s^-$ tuples.

Let $T$ be a legal-cover of $L_n$. The classification of $T$ will be $C(T) = (L^+_T, L^+_T, R^+_T, R^+_T) \in P$ where

$$\forall 0 \leq i \leq s^+, L^+_T(i) = \text{ID}_T(i)$$
$$R^+_T(i) = \text{OD}_T(n - 1 - i),$$
$$\forall 0 \leq i < s^-, L^-_T(i) = \text{ID}_T(n - 1 - i),$$
$$R^-_T(i) = \text{OD}_T(i).$$

If $T$ is not a legal-cover then we will use the convention that $C(T) = 0$. Finally, set

$$\mathcal{L}(n) = \{T \subseteq E_L(n) : T \text{ is a legal cover of } L_n\}$$
$$\mathcal{X}(n) = \{T \in \mathcal{L}(n) : C(T) = X\}$$
$$T_X(n) = |\mathcal{X}(n)|$$

so $T_X(n)$ is the number of legal-covers of $L_n$ with classification $X$.

The main reason for introducing these definitions is that checking whether a legal cover $T$ of $L_n$ can be completed to a cycle-cover of $C_n$ doesn’t depend upon all of $T$ but only on its classification $C(T)$. Furthermore, how a legal-cover in $L_n$ expands to a legal cover in $L_{n+1}$ will also only depend upon $C(T)$.

Lemma 3.2. See Figures 3 and 4.

(a) Let $X = (L^+_X, L^+_X, R^+_X, R^+_X) \in P$ and $S \subseteq \text{Hook}(n)$. Let $T$ be a legal cover in $L_n$ with $C(T) = X$.

Then whether $T \cup S$ is a cycle cover of $C_n$ depends only upon $X$ and $S$ (and not at all on $n$). In particular, if $T$ is a legal-cover of $L_n$ and $T'$ is a legal cover of $L_n$ with $C(T) = C(T')$ then

$$T \cup S \text{ is a cycle-cover of } C_n$$
$$\iff$$

$$T' \cup S \text{ is a cycle-cover of } C_n.$$

Note: We will write $X \cup S$ is a cycle cover to denote that $T \cup S$, with $C(T) = X$, is a cycle cover.

(b) Let $T'$ be a legal cover in $L_n$ with $C(T') = X' \in P$, and $S \subseteq \text{New}(n)$.

Then whether $C(T' \cup S) = X$ depends only upon $X'$ and $S$ (and not at all on $n$). In particular, if $T'$ is a legal-cover of $L_n$ and $T''$ is a legal cover of $L_n$ with $C(T') = C(T'')$ then

$$C(T' \cup S) = C(T'' \cup S)$$

Note: We will write $(X' \cup S) = X$ to denote that, when $C(T') = X'$, $C(T' \cup S) = X$.

Proof. To prove (a) recall that $T \cup S$ is a legal-cover of $L_n$ if and only if,

$\forall v \in V, \text{ID}_{T \cup S}(v) = \text{OD}_{T \cup S}(v) = 1$ or

$\forall v \in V, \text{ID}_S(v) = 1 - \text{ID}_T(v)$ and $\text{OD}_S(v) = 1 - \text{OD}_T(v)$

(3.7)
Note that $\beta$ are constants that can be mechanically calculated. Then Lemmas 3.1 and 3.2 immediately imply our main technical result, which is equivalent to (1.2).

**Lemmas 3.1 and 3.2**

For $X, X' \in \mathcal{P}$, $S \subseteq \text{Hook}(n)$ and $S' \subseteq \text{New}(n)$ set

$$\beta_{X,S} = \begin{cases} 1 & \text{if } X \cup S \text{ is a cycle cover} \\ 0 & \text{otherwise} \end{cases}$$

and

$$\alpha_{X,X',S'} = \begin{cases} 1 & \text{if } C(X' \cup S') = X \\ 0 & \text{otherwise} \end{cases}.$$  

Now set

$$\beta_X = \sum_{S \subseteq \text{Hook}(n)} \beta_{X,S}$$

and

$$\alpha_{X,X'} = \sum_{S' \subseteq \text{New}(n)} \alpha_{X,X',S'}.$$ 

Figure 3: All of the figures are in $C_6^{-1,0,2}$. Dashed edges are $\text{Hook}(n)$. The solid plus dashed edges are three different cycle covers $CC_i$, $i = 1, 2, 3$ in $C_6$. Removing the dashed $\text{Hook}(n)$ edges leaves three legal covers $T_i$, $i = 1, 2, 3$, in $L_6$. Note that $s^+ = 2$ and $s^- = 1$ so classifications are of the form $(L^+_X, L^+_X, R^+_X, R^+_X)$ where $L^+_X$ and $R^+_X$ are pairs and $L^-_X$ and $R^-_X$ are singletons. Calculation gives $C(T_1) = C(T_2) = X'_1 = (1, 0, 0, 1, 0, 1)$ and $C(T_3) = X'_3 = (0, 0, 1, 1)$. 

Figure 4: $n$ was increased from 6 to 7 and $S = \{(4, 6)\} \subseteq \text{New}(6)$ was added to the $T_i$ of the previous figure. Note that, in $L_7$, $C(T_1 \cup S) = C(T_2 \cup S) = \emptyset$ since they are no longer legal covers. Also, $C(T_3 \cup S) = X'_3(= X'_3) = (0, 0, 1, 1, 1)$. Thus, $C(X'_1 \cup S) = \emptyset$ and $C(X'_3 \cup S) = X'_3$. 

From Lemma 2.1 and the definition of a legal cover we have that this is true if and only if

$$\forall i \leq s^+, \quad \text{ID}_{S}(i) = 1 - L^X_{X} (i),$$

$$\forall i \leq s^-, \quad \text{OD}_{S}(i) = 1 - L^X_{X} (i),$$

$$\forall i \leq s^-, \quad \text{ID}_{S}(n - 1 - i) = 1 - L^X_{X} (i),$$

$$\forall i \leq s^-, \quad \text{OD}_{S}(n - 1 - i) = 1 - L^X_{X} (i).$$

and this is only dependent upon $X$ and $S$ and not upon $n$ or any other properties of $T$.

The proof of (b) is similar and omitted here. 

**Lemma 3.3.** 

Let $m = |\mathcal{P}| = 2^s$. Take any arbitrary ordering of $\mathcal{P}$ and define the $1 \times m$ constant vector $\beta = (\beta_X)_{X \in \mathcal{P}}$ and $m \times m$ constant matrix $A = (\alpha_{X,X'})_{X,X' \in \mathcal{P}}$. Finally, set $T(n) = \text{col}(T_X(n))_{X \in \mathcal{P}}$ to be a $m \times 1$ column vector. Then, Lemma 3.3 is exactly equation (1.2) which immediately implies that $T(n)$ satisfies a fixed-degree constant coefficient recurrence relation where the degree of the recurrence is at most the degree of any polynomial $P(x)$ such that $P(A) = 0$. By the Cayley-Hamilton theorem, $Q(A) = 0$, $Q(x)$ is the degree $m = 2^s$ characteristic polynomial $Q(x) = \det(IX - A)$.

We will now see that it is possible to reduce this degree from $2^s$ down to below $2^s$. 

**Lemma 3.4.** Let $A = (\alpha_{X,X'})$. Then there is a degree $2^s - 1$ polynomial $P(x)$ such that $P(A) = 0$.

**Proof.** Recall that $\bar{s} = s^+ + s^-$. Suppose $X = (L^+_X, L^+_X, R^+_X, R^+_X)$ and $X' = (L^+_X, L^+_X, R^+_X, R^+_X)$. 

Recall that $\alpha_{X,X'} = \sum_{S' \subseteq \text{New}(n)} \alpha_{X,X',S'}$ where $\alpha_{X,X',S'} = 1$ if and only if $C(X' \cup S) = X$, and is otherwise 0. 

Now let $L_+$, $L_-$ be any $2^s$ and $2^s$ binary tuples and partition $\mathcal{P}$ up into $2^s$ sets of size $2^s$, $\mathcal{P}_{L_+,L_-} = \{X \in \mathcal{P} : L^+_X = L_+, L^+_X = L_- \}$. 

\[
T(n) = \sum_{X \in \mathcal{P}} \beta_X T_X(n) \\
and \\
T_X(n + 1) = \sum_{X' \in \mathcal{P}} \alpha_{X,X'} T(n).
\]
Note that, if $S \subseteq \mathbf{New}(n)$, none of $S$’s edges have endpoints in $L^+(n)$ or $L^-(n)$. Intuitively, this is because edges in $\mathbf{New}(n)$ only connect vertices near the right side of the lattice and do not touch any vertices on the left side of the lattice.

Thus, if $\alpha_{X,X',S} = 1$, then $L^X = L^X'$ and $L^X = L^X'$. In particular this means that if $\alpha_{X,X',S} = 1$ then $X, X'$ are both in the same partition set $P_{L^+L^-}$.

Now suppose that $\alpha_{X,X',S} = 1$. Let $L_+, L_-$ be any other $2^{s^+}$ and $2^{s^-}$ binary tuples and set

\[ \tilde{X} = (L_+, L_-, R^X_+, R^X_-) \text{ and } \tilde{X}' = (L_+, L_-, R^{X'}_+, R^{X'}_-) \quad (3.8) \]

Then, again using the fact that none of the endpoints of $S$ are in $L^+(n)$ or $L^-(n)$ we have that $C(X' \cup S) = \tilde{X}'$ if and only if $C(X' \cup S) = \tilde{X}$ so $\alpha_{X,X'} = \alpha_{X,X'}$.

When constructing matrix $A = (\alpha_{X,X'})_{X,X' \in \mathcal{P}}$ we previously allowed any arbitrary ordering of $\mathcal{P}$. Now order the $X \in \mathcal{P}$ lexicographically; this groups all of the $X$ in a particular $P_{L^+L^-}$ consecutively. The observations above imply that $A$ is partitioned into $2^s \times 2^s$ blocks where each block is of size $2^s \times 2^s$. The non-diagonal blocks correspond to $\alpha_{X,X'}$ where $X, X'$ are in different partitions so all of the non-diagonal blocks are 0. On the other hand, the fact that $\alpha_{X,X'} = \alpha_{X,X'}$ for the $X, X'$ defined in (3.8), tells us that all the diagonal blocks are copies of each other.

Let $\tilde{A}$ be one of the $2^s \times 2^s$ diagonal blocks in $A$. $A$ can then be denoted as $A = \text{diag} (\tilde{A}, \tilde{A}, \ldots, \tilde{A})$ where $\tilde{A}$ contains $2^s$ copies of $\tilde{A}$ on its diagonal. Thus, $\forall i, A^i = \text{diag}(A^i, A^i, \ldots, A^i)$. In particular, this means that any polynomial $P(x)$ that annihilates $\tilde{A}$ also annihilates $A$. Since $\tilde{A}$ is a $2^s \times 2^s$ matrix, the Cayley-Hamilton theorem says that the characteristic polynomial $\tilde{P}(x)$ of $\tilde{A}$, which is of degree $2^s$, annihilates $\tilde{A}$.

By a more careful analysis of the structure of $\tilde{A}$ it is possible to show that $\tilde{P}(x)$ actually has degree $2^s - 1$ but, as mentioned in the introduction, that further analysis will be omitted here.

Lemma 3.3 tells us that (1.2) holds while Lemma 3.4 tells us that matrix $A$ is annihilated by polynomial $P(x)$ of degree $2^s - 1$. Combining them gives that $T(n)$ satisfies a degree-$2^s - 1$ constant coefficient recurrence relation. In order to actually derive the recurrence relation, though, it is necessary to calculate the $\alpha_{X,X'}$, $\beta_X$, $\tilde{T}$ and $P$ as well as the first $2^s - 1$ values of $T(n) = \beta T(n)$. It is relatively straightforward (but omitted in this extended abstract) to see how to evaluate all of these in $O(s2^{5s})$ time by evaluating $O(2^{2s})$ permanents of size $2s$ and $O(2^{4s})$ of size $s$.

We just saw how to calculate the number of cycle-covers in constant-jump circulant graphs. Reviewing the proof, everything followed directly as a consequence from the recursive decomposition of circulant graphs in (2.3) combined with the structural properties of the decomposition given in Lemma 2.1. But, as also derived in Section 2, non-constant jump circulants have exactly the same structural properties, given in (2.5) and Lemma 2.2. Therefore, the entire proof developed in Section 3 can be rewritten for non-constant jump circulants. The only difference is in the degree of the recurrence relation for the number of cycle-covers. Reviewing the proof for the constant-jump case we can see that the order of the recurrence relation is really $2^{|R^+(n)| + |R^-(n)|}$ which worked out to $2^s - 1$. In the non-constant case, from Lemma 2.2, we can calculate that $|R^+(n)| + |R^-(n)| = p(|s| + s^+ + s^-) + 2s$ so the order of the recurrence relation will then be $2^{p(|s| + s^+ + s^-) + 2s}$. Note that in the constant jump case we had $p = s = 0$ so this collapses down to $2^{s^+ + s^-} = 2^s$ which is what we had previously derived. For an example of such a recurrence relation, see the second set of graphs in Table 1.

References


As discussed in the paper we have that
\[ T_L \text{ number of cycle covers in } \beta \]

A Worked example for \( C_n^{1,2} \)
As discussed in the paper we have that \( T(n) \), the number of cycle covers in \( C_n^{1,2} \), satisfies
\[ \forall n \geq 2s, \quad T(n) = \beta T(n) \quad \text{and} \quad T(n + 1) = A T(n) \]
where \( \beta = (\beta_X)_{X \in \mathcal{P}} \) and \( A = (\alpha_{X,X'})_{X,X' \in \mathcal{P}} \).

For \( C_n^{1,2} \) we have \( s^+ = 2, s^- = 0 \) so \( s = s^+ + s^- = 2 \). Definition 3.2 then says that every \( X \in \mathcal{P} \) is in the form \( X = (L^X_+, L^X_-, R^X_-, R^X_+) \) where \( L^X_+, R^X_+ \in \{0, 1\}^2 \) and \( L^X_-, R^X_- \) are empty. We can therefore represent every \( X \) by a four-bit binary vector in which the first two bits represent \( L^X_+ \) and the last two \( R^X_- \); there are 16 such \( X \in \mathcal{P} \). Ordering the \( X \) lexicographically we calculate that \( \beta \) is
\[
(1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 )
\]
\( \bar{T}(4) \) is
\[
(1 \ 0 \ 0 \ 0 \ 0 \ 2 \ 1 \ 0 \ 0 \ 3 \ 2 \ 0 \ 0 \ 0 \ 0 \ 1 )^T
\]
(where the \( t \) denotes taking the transpose), and Transfer matrix \( A(X) \) is
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{pmatrix}
\]
As predicted by Lemma 3.4, \( A \) is partitioned into 16 \( 4 \times 4 \) blocks where all but the diagonal blocks are 0 and all of the diagonal blocks are equal to some \( 4 \times 4 \) matrix \( \bar{A} \) which in this case is
\[
\bar{A} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix}
\]
This means that
\[
Q(x) = \det(Ix - \bar{A}) = (x^2 - x - 1)(x - 1)^2,
\]
the characteristic polynomial of \( \bar{A} \), annihilates \( A \).

Working through the details we can then solve to find that \( C_n^{1,2} = 2T(n - 1) - T(n - 3) \) with initial values \( T(4) = 9, T(5) = 13, \) and \( T(6) = 12. \)

B Other Applications
In this appendix we quickly mention two other applications of the technique introduced in this paper.

The first is in analyzing the number of cycles in certain classes of random restricted permutations. Using the standard cycle-decomposition of a permutation there is 1-1 correspondence between permutations...
\( T_1(n) = 3T(n-1) - T_1(n-2) - 3T_1(n-3) + T_1(n-4) + T_1(n-5) \)

initial values 22, 42, 80, 149, 274

for \( n = 4, 5, 6, 7, 8 \)

\( T_1(n) \sim \frac{\phi^n}{\phi + \phi^2} \)

\( \frac{T_1(n)}{T_0(n)} \sim .7236n^\phi \)

\( C_0^{1.2} \)

\( T_1(n) = 3T(n-1) - 6T_1(n-3) + 2T_1(n-4) + 4T_1(n-5) - T_1(n-6) - T_1(n-7) \)

initial values 21, 32, 56, 93, 161, 275, 475

for \( n = 4, 5, \ldots, 10 \)

\( T_1(n) \sim \frac{\phi^2}{\phi + \phi^2} n^\phi \)

\( \frac{T_1(n)}{T_0(n)} \sim .2764n^\phi \)

Table 2: \( T_1(n) \) is the number of cycles in the given graph with \( n \) vertices.

\( \pi \in S_n \) and cycle-covers of the complete directed graph on \( n \)-vertices. For given parameters \( p, s, p_i, s_i \) and \( S \) as in Definition 1.4 define

\[ S_{pn+s}(S) = \{ \pi \in S_{pn+s} : \pi[i] - i \mod (pn + s) \in S \} \]

(2.9)

to be the set of permutations in which \( \pi[i] \) is restricted by (2.9). Now suppose that we pick a permutation \( \pi \) uniformly at random from \( S_{pn+s}(S) \) and set \( X = \# \) of cycles in \( \pi \). What can be said about the distribution of \( X \)?

By the 1-1 correspondence between permutations and cycle-covers, \( \pi \in S_{pn+s}(S) \) if and only if the corresponding cycle-cover is in \( C_n \). Thus, the number of such permutations satisfies \( |S_{pn+s}(S)| = T(n) \) where \( T(n) \) is the number of cycle-covers in \( C_n \). Suppose now that for cycle cover \( T \in CC(n) \) we define \( \#_C(T) \) to be the number of cycles composing cover \( T \) and set

\[ TC_i(n) = \sum_{T \in CC(n)} (\#_C(T))^i \]

That is, \( TC_0(n) = T(n) \) while \( TC_1(n) \) is the total number of cycles summed over all cycle-covers in \( C_n \). Then, again by the correspondence, we have that the moments of \( X \) are given by

\[ \forall i \geq 0, \ E(X^i) = \frac{TC_i(n)}{TC_0(n)}. \]

The interesting point is that the transfer matrix approach introduced in this paper can mechanically be extended to counting the total number of cycles in the cycle-covers, to show that for every \( i, TC_i(n) \) satisfies a fixed-order constant coefficient recurrence relation. For given \( p, s, p_1, p_2, \ldots, p_k \) and \( s_1, s_2, \ldots, s_k \) this permits, for example, calculating \( E(X) \) and \( Var(X) \).

As an illustration recall the results from Table 1 counting the number of cycle covers in \( C_n^{1.0.1} \) and \( C_n^{0.1.2} \). Even though these two graphs are not isomorphic they had the same number of cycle-covers because the adjacency matrix of the second is just the adjacency matrix of the first with every row (cyclicly) shifted over one step. Since permanents are invariant under cyclic shifts both matrices have the same permanent which is \( \sim \phi^n \) where \( \phi = (1 + \sqrt{3})/2 \).

Using our technique we calculated \( TC_1(n) \) for both cases with the results given in Table 2.

In both cases we have that \( TC_1(n) \sim cn^\phi \). This means that if a permutation on \( n \) items is chosen at random from the corresponding distribution then, on average, it will have \( \frac{T_1(n)}{T_0(n)} \sim cn \) cycles. It is interesting to note that that \( c \) is different for the two cases.

The second application of the technique we note is that a minor modification permits using it to show that the number of Hamiltonian Cycles in a directed circulant graph \( C_n \) also satisfies a constant-coefficient recurrence relation in \( n \). This fact was previously known for undirected circulant graphs \([9, 10]\) but doesn’t seem to have been known for directed circulants, with the exception of the special case of in(out)-degree 2 circulants \([20]\).