STIRLING FUNCTIONS AND A GENERALIZATION OF WILSON’S THEOREM

MATTHEW A WILLIAMS

ABSTRACT. For positive integers $m$ and $n$, denote $S(m, n)$ as the associated Stirling number of the second kind and let $z$ be a complex variable. In this paper, we introduce the Stirling functions $S(m, n, z)$ which satisfy $S(m, n, z) = S(m, n)$ for any $z$ which lies in the zero set of a certain polynomial $P_{(m,n)}(z)$. For all real $z$, the solutions of $S(m, n, z) = S(m, n)$ are computed and all real roots of the polynomial $P_{(m,n)}(z)$ are shown to be simple. Applying the properties of the Stirling functions, we investigate the divisibility of the numbers $S(m, n)$ and then generalize Wilson’s Theorem.

Preliminaries and Notation

For brevity, we will denote $\mathbb{Z}_+ = \mathbb{N}\setminus\{0\}$, $\mathbb{E} = 2\mathbb{Z}_+$ and $\mathbb{O} = \mathbb{Z}_+\setminus\mathbb{E}$. If $P$ is a univariate polynomial with real or complex coefficients, define $Z(P) = \{z \in \mathbb{C} : P(z) = 0\}$ and $Z_{\mathbb{R}}(P) = Z(P) \cap \mathbb{R}$. Throughout, it will be assumed that $m, n \in \mathbb{Z}_+$ and $d := m - n$. In agreement with the notation of Riordan [3], $s(m,n)$ and $S(m,n)$ will denote the Stirling numbers of the first and second kinds, respectively. We will also use the notation $B(m,n) = n!S(m,n)$. Although we are mainly concerned with the numbers $S(m, n)$, one recalls that for $z \in \mathbb{C}$

$$
(z)_n = (z-1) \cdots (z-n+1) = \sum_{k=0}^{n} s(n,k) z^k.
$$

Let $p$ be prime. In connection to the divisibility of the numbers $S(m, n)$, we will use the abbreviation $n \equiv_p m$ in place of $n \equiv m \pmod{p}$. Note that $\nu_p(n) := \max\{\kappa \in \mathbb{N} : p^\kappa | n\}$ ($\nu_p(n)$ is known as the $p$-adic valuation of $n$). If $n = \sum_{k=0}^{n} b_k 2^k$ ($b_k \in \{0, 1\}$, $b_m = 1$) is the binary expansion of $n$, let $n_2$ denote the binary representation of $n$, written $b_m \cdots b_0$, where $(n_2)_k := b_k$ and $m$ is called the MSB position of $n_2$. We will call an infinite or $n \times n$ square matrix $A = [a_{ij}]$ Pascal if for every $i, j$,

$$
a_{ij} = \binom{i+j}{j} \quad \text{or} \quad a_{ij} = \binom{i+j}{j} \pmod{p}.
$$

We note that if $A \in \mathbb{N}^{n \times n}$ is Pascal, then $A$ is symmetric and $\det(A) \equiv_p 1$ [5]. Finally, for the sake of concision, we will make use of the map $e : \mathbb{Z}_+ \to \mathbb{E}$ such that

$$
e(n) = \begin{cases} n & \text{if } n \in \mathbb{E} \\ n+1 & \text{otherwise}. \end{cases}
$$

Following these definitions, let us introduce the Stirling functions:

$$
S(m, n, z) = \frac{(-1)^d}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^k (z-k)^m.
$$

It is known [1] that $S(m, n, z) = S(m, n)$ if $d \le 0$. The aim of this paper is to show that $d > 0$ implies $S(m, n, z) = S(m, n)$ for real $z$ only if $z \in \{0, n\}$ (Corollary 3), to investigate...
the $p$-adic valuation and parity of the numbers $S(m, n)$, and to formulate and prove a generalization of Wilson's Theorem (Proposition 14).

1. **The Real Solutions of** $S(m, n, z) = S(m, n)$.

We first observe a classical formula from combinatorics [1]:

**Theorem 1.** The number of ways of partitioning a set of $m$ elements into $n$ nonempty subsets is given by

\[ S(m, n) = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)^m. \]

It was discovered independently by Ruiz [1,2] that

\[ S(n, n) = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^k (z-k)^n \quad (z \in \mathbb{R}). \]

Indeed, (2) is an evident consequence of the Mean Value Theorem. Katsuura [1] noticed that (2) holds even if $z$ is an arbitrary complex value, as did Vladimir Dragovic (independently). The following proposition extends (2) to the case $d > 0$.

**Proposition 1.** The equation $S(m, n, z) = S(m, n)$ holds for all $z \in \mathbb{C}$ if $d \leq 0$, and for only the roots of the polynomial

\[ P_{(m,n)}(z) = \sum_{j=1}^{d} \binom{m}{j} S(m-j, n)(-z)^j \]

in the case $d > 0$.

**Proof.** Let $z \in \mathbb{C}$. One easily verifies that

\[ \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^k (z-k)^m = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^k \sum_{j=0}^{m} \binom{m}{j} z^j (-k)^{m-j} \]

\[ = (-1)^d \sum_{j=0}^{m} \binom{m}{j} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^{m-j} \]

\[ (-z)^j. \]

In view of Theorem 1, we have by symmetry

\[ (-1)^d \sum_{j=0}^{m} \binom{m}{j} \left[ \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^{m-j} \right] (-z)^j \]

\[ = (-1)^d \sum_{j=0}^{m} \binom{m}{j} S(m-j, n)(-z)^j \]

(3)

Hence by (3)

\[ S(m, n) = S(m, n, z) = P_{(m,n)}(z). \]

Now by the definition of $P_{(m,n)}(z)$ and (4), $d \leq 0$ implies $S(m, n) = S(m, n, z)$ for every $z \in \mathbb{C}$. Conversely, if $d > 0$, then $P_{(m,n)}(z)$ is of degree $d$ and by (4) $S(m, n) = S(m, n, z)$ holds for $z \in \mathbb{C}$ if, and only if, $z \in \mathbb{Z}(P_{(m,n)})$. This completes the proof. \[ \square \]

In contrast to the case $d \leq 0$, we now have:
Corollary 1. If $d > 0$, there are at most $d$ distinct complex numbers $z \in \mathbb{C}$ such that

$$S(m, n, z) = S(m, n).$$

Proof. Noting that $d > 0$ implies $\deg(P_{m,n}) = d$, the Corollary follows by the Fundamental Theorem of Algebra. □

Remark 1. In view of the definition of $P_{m,n}(z)$, $z = 0$ is a root of this polynomial whenever $d > 0$. Proposition 1 then implies that $S(m, n, 0) = S(m, n)$ for every $m, n \in \mathbb{Z}_+$. Now if $d \in \mathbb{E}$, we have that

$$S(m, n, n) = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} (n-k)^m = S(m, n)$$

by Theorem 1. Thus, $P_{m,n}(n) = 0$ whenever $d \in \mathbb{E}$ by equation (4).

The next series of Propositions provides the calculation of $Z_R(P_{m,n})$.

Proposition 2. If $d > 0$, then the following assertions hold:

(A) $d \in \mathbb{D}$ implies $z = 0$ is a simple root of $P_{m,n}(z)$.

(B) $d \in \mathbb{E}$ implies $z = 0$ and $z = n$ are simple roots of $P_{m,n}(z)$.

(C) All real roots of $P_{m,n}(z)$ lie in $[0, n]$.

Proof. Note that by a formula due to Gould [3, Eqn. 2.57], we have

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k (z-k)^m = \sum_{j=0}^{d} \binom{z-n}{j} B(m, n+j).$$
Now by the above and equation (4), we obtain an expansion of $P_{(m,n)}(z)$ at $z = n$:

$$P_{(m,n)}(z) = \frac{(-1)^d}{n!} \sum_{j=0}^{d} \binom{n+j}{j} B(m, n+j) - S(m, n) = \frac{(-1)^d}{n!} \sum_{j=1}^{d} \binom{n+j}{j} S(m, n+j)(z-n)_j + ((-1)^d - 1)S(m, n) = \frac{(-1)^d}{n!} \sum_{j=1}^{d} \left[ \sum_{q=j}^{d} \binom{n+q}{n} S(m, n+q)S(q, j) \right] (z-n)_j + ((-1)^d - 1)S(m, n).$$

Let $1 \leq j \leq d$. We differentiate each side of (4) to get

$$P_{(m,n)}^{(j)}(z) = \frac{(-1)^d}{n!} \sum_{k=0}^{n} \binom{n}{k} (-1)^k (z-k)^{m-j}. \quad (6)$$

We have by (6) and Theorem 1

$$P_{(m,n)}^{(j)}(0) = (-1)^j (m)_j S(m-j, n), \quad P_{(m,n)}^{(j)}(n) = (-1)^d (m)_j S(m-j, n), \quad (7)$$

hence (A) and (B) follow by Remark 1 and (7). Now, notice that applying (7) to (5) yields the convolution identity

$$\sum_{q=j}^{d} \binom{n+q}{n} S(m, n+q)S(q, j) = \binom{m}{j} S(m-j, n) \quad (1 \leq j \leq d). \quad (8)$$

Observing that $P_{(m,n)}(z) > 0$ if $z < 0$, applying (8) to (5) yields

$$z \in (-\infty, 0) \cup (n, \infty) \Rightarrow |P_{(m,n)}(z)| > 0.$$

Assertion (C) is now established, and the proof is complete. \qed

As can be seen above, by (5) and (8) we have that

$$P_{(m,n)}(z) = \sum_{j=1}^{d} \binom{m}{j} S(m-j, n)(-z)^j$$

$$= (-1)^d P_{(m,n)}(n-z) + ((-1)^d - 1)S(m, n). \quad (9)$$

Therefore, by (4) and (9), one obtains through successive differentiation:

**Proposition 3.** Let $d > 0$ and $k \in \mathbb{Z}_+$. Then, we have that

$$S^{(k)}(m, n, z) = P_{(m,n)}^{(k)}(z) = (-1)^{d-k} P_{(m,n)}^{(k)}(n-z) = (-1)^{d-k} S^{(k)}(m, n, n-z).$$

Thus, the derivatives of $P_{(m,n)}(z)$ and $S(m, n, z)$ are symmetric about the point $z = n/2$.

Further, the functions $S(m, n, z)$ have the following recursive properties:

**Proposition 4.** Let $m, n \geq 2, d > 0$ and $1 \leq k \leq d + 1$. Then, we have:

(A) $S(m, n, z) = S(m-1, n-1, z-1) - zS(m-1, n, z)$

(B) $S^{(k)}(m, n, z) = (-1)^k (m)_k S(m-k, n, z).$
Proof. It is easily verified that
\[
S(m, n, z) = (-1)^d \left( z \sum_{k=0}^{n} \binom{n}{k} (-1)^k (z - k)^m - 1 + \sum_{k=0}^{n} \frac{n!(-1)^{k+1}(z - k)^{m-1}}{(k - 1)!(n - k)!} \right)
\]
\[
= -zS(m - 1, n, z) + \frac{(-1)^d}{(n - 1)!} \sum_{k=0}^{n-1} \binom{n - 1}{k} (-1)^k (z - 1 - k)^{m-1}
\]
\[
= -zS(m - 1, n, z) + S(m - 1, n - 1, z - 1)
\]
which establishes (A). To obtain (B), differentiate the Stirling function \(S(m, n, z)\) \(k\) times and apply the definition of \(S(m - k, n, z)\). \(\square\)

Remark 2. Let \(d > 0\) and \(k \in \mathbb{Z}_+\). By Propositions 3 and 4B, we have that
\[
(d - k) \in \mathbb{O} \Rightarrow P^{(k)}_{(m, n)}(n/2) = 0 = S(m - k, n, n/2).
\]

Now suppose \((d - k) \in \mathbb{E}\). In this case, Propositions 3 and 4B do not directly reveal the value of \(P^{(k)}_{(m, n)}(n/2)\). However, combined they imply a result concerning the sign (and more importantly, the absolute value) of \(P^{(k)}_{(m, n)}(z)\) if \(z \in \mathbb{R}\). Consider that if \(d = m - 1\),
\[
[S(m - k, 1, z) = z^{m-k} - (z - 1)^{m-k} > 0] \iff [z > z - 1] \quad (z \in \mathbb{R})
\]
since \((m - k) \in \mathbb{O}\). Proceeding inductively, we obtain:

Proposition 5. Suppose \(d \in \mathbb{E}\). Then, \(S(m, n, z) > 0\) holds for every \(z \in \mathbb{R}\).

Proof. The Proposition clearly holds in the case \(n = 1\). If also for \(n = N\), let \(m\) be given which satisfies \((m - (N + 1)) \in \mathbb{E}\). Set \(N + 1 = N'\). We expand \(S(m, N', z)\) at \(z = N'/2\) to obtain
\[
S(m, N', z) = \sum_{j=0}^{m-N'} \frac{S^{(j)}(m, N', N'/2)}{j!} \left( z - \frac{N'}{2} \right)^j.
\]
Now, consider that by Propositions 4A and 4B we have that
\[
S^{(j)}(m, N', \frac{N'}{2}) = (-1)^j (m - j) S^{(j)}(m - j, N', \frac{N'}{2})
\]
(12)
\[
= (-1)^j (m) \left[ S^{(m - j - 1, N, \frac{N'}{2} - 1)} - \frac{N'}{2} S^{(m - j - 1, N', \frac{N'}{2})} \right]
\]
for \(0 \leq j \leq m - N'.\) Hence by (10), (12) and the induction hypothesis
\[
S^{(j)}(m, N', \frac{N'}{2}) = (-1)^j (m) S^{(m - j - 1, N, \frac{N'}{2} - 1)} > 0 \quad (j \in \mathbb{N} \setminus \mathcal{O}, \ j < m - N' - 1)
\]
and by Proposition 1
\[
S^{(m - N')}(m, N', \frac{N'}{2}) = (-1)^{m - N'} (m) S^{(m - N', N', \frac{N'}{2})} = (m)_{m - N'} > 0.
\]
Thus \(S(m, N', z)\) may be written as
\[
S(m, N', z) = \sum_{j=0}^{m - N'} \frac{S^{(2j)}(m, N', N'/2)}{(2j)!} \left( z - \frac{N'}{2} \right)^{2j}
\]
where each coefficient of the above expansion at \(z = \frac{N'}{2}\) is positive. Since \(m\) is arbitrary, the Proposition follows by induction. \(\Box\)

![Figure 3](image.png)

**Figure 3.** Plots of \(S(6, 4, z)\), \(S(8, 4, z)\) and \(S(10, 4, z)\). Note that each function achieves its global minimum (a positive value) at \(z = 2\).

**Corollary 2.** Let \(k \in \mathbb{Z}_+\). Then, \(|P_{(m, n)}^{(k)}(z)| > 0\) holds for every \(z \in \mathbb{R}\) if \((d - k) \in \mathcal{E}\).

**Proof.** Assume the hypothesis. By Propositions 3 and 4B, one obtains
\[
|P_{(m, n)}^{(k)}(z)| = (m)_k |S(m - k, n, z)|.
\]
Noting \(S(m - k, n, z) > 0\) if \(z \in \mathbb{R}\) by Proposition 5, the Corollary is proven. \(\Box\)
Remark 3. We now calculate $Z_{\mathbb{R}}(P_{(m,n)})$ by Corollary 2 and the use of Rolle’s Theorem. Sharpening Corollary 1, Proposition 6 (below) asserts that there are at most two distinct real solutions of the equation $S(m,n,z) = S(m,n)$ if $d > 0$, dependent upon whether $d \in \mathbb{E}$ or $d \in \mathbb{O}$. This result is in stark contrast to the Theorem of Ruiz, which has now been generalized to a complex variable (Proposition 1).

Proposition 6. Let $d > 0$. Then, $Z_{\mathbb{R}}(P_{(m,n)}) \subseteq \{0, n\}$.

Proof. By Proposition 2, we may assume $d > 2$. If $d \in \mathbb{E}$, Corollary 2 implies that

$$|P^{(2)}(m,n)(z)| > 0 \quad (z \in \mathbb{R}).$$

Hence $|Z_{\mathbb{R}}(P’_{(m,n)})| \leq 1$. Proposition 2 now gives $Z_{\mathbb{R}}(P_{(m,n)}) = \{0, n\}$ (for otherwise, Rolle’s Theorem assures $|Z_{\mathbb{R}}(P’_{(m,n)})| > 1$). Now if $d \in \mathbb{O}$, Corollary 2 yields

$$|P’_{(m,n)}(z)| > 0 \quad (z \in \mathbb{R})$$

and thus $|Z_{\mathbb{R}}(P_{(m,n)})| \leq 1$. We now conclude by Proposition 2 that $Z_{\mathbb{R}}(P_{(m,n)}) = \{0\}$, which completes the proof. □

Corollary 3. If $d > 0$, the only possible real solutions of

$$S(m,n,z) = S(m,n)$$

are $z = 0$ and $z = n$. Moreover, for $d > 2$ there exist $z \in \mathbb{C} \setminus \mathbb{R}$ which satisfy the above.

Proof. The first assertion is a consequence of Propositions 1 and 6. Now without loss, assume $d > 2$. By Propositions 2 and 6, there are at most two real roots of $P_{(m,n)}(z)$. Since we have that $\deg(P_{(m,n)}) > 2$, by the Fundamental Theorem of Algebra we obtain $Z_{\mathbb{R}}(P_{(m,n)}) \subseteq Z(P_{(m,n)})$ which implies the existence of $z \in \mathbb{C} \setminus \mathbb{R}$ such that $P_{(m,n)}(z) = 0$. The Corollary now follows by Proposition 1. □

2. Some Divisibility Properties of the Stirling Numbers of the Second Kind

Let $d > 0$. By (10), we expand the Stirling functions $S(m,n,z)$ at $z = n/2$ as follows:

$$d \in \mathbb{E} \Rightarrow S(m,n,z) = \sum_{j=0}^{d/2} \binom{m}{2j} S\left(m - 2j, n, \frac{n}{2}\right) \left(z - \frac{n}{2}\right)^{2j} \quad (13)$$

$$d \in \mathbb{O} \Rightarrow S(m,n,z) = -\sum_{j=0}^{d-1} \binom{m}{2j + 1} S\left(m - 2j - 1, n, \frac{n}{2}\right) \left(z - \frac{n}{2}\right)^{2j+1}. \quad (14)$$

Now if $d \in \mathbb{E}$, (13) and Proposition 5 imply that $S(m,n,z) \geq S(m,n,n/2) > 0$ for every $z \in \mathbb{R}$. Conversely, if $d \in \mathbb{O}$, (14) implies that $Z_{\mathbb{R}}(S(m,n,z)) = \{n/2\}$ (apply similar reasoning as that used in Proposition 6). Thus we introduce the numbers:

$$v(m,n) := \min_{z \in \mathbb{R}} |S(m,n,z)|.$$

Taking $z = 0$ in (13) and (14), it follows by Propositions 1 and 2 that

$$d \in \mathbb{E} \Rightarrow S(m,n) = \sum_{j=0}^{d/2} \binom{m}{2j} v(m - 2j, n) \left(n \right)^{2j} \quad (15)$$

$$d \in \mathbb{O} \Rightarrow S(m,n) = -\sum_{j=0}^{d-1} \binom{m}{2j + 1} v(m - 2j - 1, n) \left(n \right)^{2j+1}. \quad (16)$$
Using the formulas (15) and (16) combined with Proposition 7 (formulated below), we may deduce some divisibility properties of the numbers $S(m, n)$. These include lower bounds for $\nu_p(S(m, n))$ if $d \in O$ and $p | e(n)/2$, and an efficient means of calculating the parity of $S(m, n)$ if $d \in E$.

**Proposition 7.** Let $n \in E$. Then, $v(m, n) \in \mathbb{Z}$ whenever $d > 0$.

**Proof.** In view of (10), we may assume without loss that $d \in E$. Set $q = n/2$. By (15) and Proposition 1 we have that

\[
S(n + 2, n) = v(n + 2, n) + \binom{n + 2}{2} v(n, n) q^2
\]

(17)

Thus, (17) furnishes the base case:

\[
v(n + 2, n) = S(n + 2, n) - \binom{n + 2}{2} q^2.
\]

Now if $d = 2k$ and $v(n + 2j, n) \in \mathbb{Z}$ for $1 \leq j \leq k$, one readily computes

\[
v(n + d + 2, n) = S(n + d + 2, n) - \sum_{j=1}^{k+1} \binom{n + d + 2}{2j} v(n + d - 2(j - 1), n) q^{2j}.
\]

(18)

Since the RHS of (18) lies in $\mathbb{Z}$ by the induction hypothesis, the Proposition follows. \qed

**Proposition 8.** Let $d \in O$ and $p$ be prime. Then, we have that

\[
\nu_p(S(m, n)) \geq \begin{cases} 
\nu_p(e(n)) - 1 & \text{if } p = 2 \\
\nu_p(e(n)) & \text{otherwise}. 
\end{cases}
\]
Proof. It is sufficient to show that \( d \in \mathcal{O} \) implies \( e(n)/2 \mid S(m, n) \). First assuming that \( n \in \mathcal{E} \), by (16) we obtain

\[
S(m, n) = \frac{n}{2} = \sum_{j=0}^{\frac{n-1}{2}} \binom{m}{2j+1} v(m-2j-1, n) \left( \frac{n}{2} \right)^{2j}.
\]

Since Proposition 7 assures the RHS of (19) lies in \( \mathbb{Z} \), \((n/2) \mid S(m, n)\) follows. Now if \( n \in \mathcal{O} \), one observes

\[
S(m, n) = S(m+1, e(n)) - e(n)S(m, e(n)).
\]

Thus, Proposition 7 and (19) imply \( e(n)/2 \mid S(m, n) \). This completes the proof. \( \square \)

**Figure 5.** The numbers \( S(m, n) \) such that \( d \in \mathcal{O} \). In the image above, each tile corresponds to an \((m, n)\) coordinate, \(1 \leq m, n \leq 50\). Dark blue tiles represent those \( S(m, n) \) such that \( d \in \mathcal{E} \cup \mathbb{Z}_{\leq 0}\). Note that the remaining tiles, corresponding to the \( S(m, n) \) such that \( d \in \mathcal{O} \), are colored according to their divisibility by \( e(n)/2 \).

**Corollary 4.** Let \( d \in \mathcal{O} \). Then \( S(m, n) \) is prime only if \( m = 3 \) and \( n = 2 \).

**Proof.** Assume the hypothesis. A combinatorial argument gives \( S(3, 2) = 3 \). If we suppose that \( 3 \mid S(2k + 1, 2) \), the identity

\[
S(2(k+1) + 1, 2) = 4S(2k + 1, 2) + 3
\]

yields \( 3 \mid S(2(k+1) + 1, 2) \). Therefore, by induction we have that \( 3 \mid S(2N + 1, 2) \) for every \( N \in \mathbb{Z}_+ \). However \( S(2N + 1, 2) > S(3, 2) \) if \( N > 1 \), and thus \( S(2N + 1, 2) \) is prime only if...
N = 1. Now, assume that n > 2. Then e(n)/2 > 1 and by Proposition 8, e(n)/2 | S(m, n).
Noting d > 0 implies
\[ S(m, n) = nS(m - 1, n) + S(m - 1, n - 1) > n > \frac{e(n)}{2} \]
it follows that S(m, n) is composite. This completes the proof. \[ \square \]

Corollary 4 fully describes the primality of the numbers S(m, n) such that d ∈ O. For those which satisfy d ∈ E, infinitely many may be prime (indeed, the Mersenne primes are among these numbers). It is however possible to evaluate these S(m, n) modulo 2, using only a brief extension of the above results (Propositions 9-13). We remark that these numbers produce a striking geometric pattern (known as the Sierpinski Gasket, Figure 6).

We now introduce
\[ \ell_n := \min\{k \in 4\mathbb{Z}_+ : k \geq n\} - 3 = 1 + 4\left\lfloor \frac{n - 1}{4} \right\rfloor. \]
The \( \ell_n \) will eliminate redundancy in the work to follow (see Proposition 9, below).

**Proposition 9.** Let d ∈ E. Then, we have that
\[ S(n + d, n) \equiv_2 S(\ell_n + d, \ell_n). \]

**Proof.** Assume without loss that n \( \neq \ell_n \). Then, there exists 1 ≤ j ≤ 3 such that n = \( \ell_n + j \).
If j = 1, then n ∈ E so that
\[ S(n + d, n) \equiv_2 S(n - 1 + d, n - 1) \equiv_2 S(\ell_n + d, \ell_n). \]
Now if j ∈ \{2, 3\}, notice 4 | e(n) and thus Proposition 8 assures 2 | S(n + (d - 1), n). Thus,
\[ S(n + d, n) \equiv_2 S(\ell_n + (j - 1) + d, \ell_n + (j - 1)). \]
Taking j = 2 then j = 3 above completes the proof. \[ \square \]

With the use of Proposition 9, it follows that for every d ∈ E
\[ 1 \equiv_2 S(1 + d, 1) \equiv_2 \cdots \equiv_2 S(4 + d, 4). \]

Before continuing in this direction, we first prove a generalization of the recursive identity
\[ S(m, n) = nS(m - 1, n) + S(m - 1, n - 1) \]
for the sake of completeness.

**Lemma 1.** Let n > 1 and d > 0. Then, for 1 ≤ k ≤ d,
\[ S(n + d, n) = n^{d-k+1}S(n + k - 1, n) + \sum_{j=0}^{d-k} n^j S(n - 1 + (d - j), n - 1) \]

**Proof.** We clearly have
\[ S(n + d, n) = n^{d-d+1}S(n + d - 1, n) + \sum_{j=0}^{d-d} n^j S(n - 1 + (d - j), n - 1). \]
Now, assume that for 1 ≤ ξ ≤ d,
\[ S(n + d, n) = n^{d-\xi+1}S(n + \xi - 1, n) + \sum_{j=0}^{d-\xi} n^j S(n - 1 + (d - j), n - 1). \]
Then, by a brief computation
\[ S(n + d, n) = n^{d-\xi+1}(nS(n + \xi - 2, n) + S(n - 1 + (\xi - 1), n - 1)) + \sum_{j=0}^{d-\xi} n^j S(n - 1 + (d - j), n - 1) \]
\[ = n^{d-(\xi-1)+1}S(n + (\xi - 1) - 1, n) + \sum_{j=0}^{d-(\xi-1)} n^j S(n - 1 + (d - j), n - 1). \]

The Lemma now follows by induction. \(\square\)

**Proposition 10 (Parity Recurrence).** Let \(d \in \mathbb{E}\) and \(n > 4\). Then, we have that
\[ S(n + d, n) \equiv_2 \sum_{j=0}^{d/2} S(\ell_{n-4} + (d - 2j), \ell_{n-4}). \]

**Proof.** In view of Proposition 9, we may assume \(n = \ell_n\). Consequently, \(\ell_{n-1} = \ell_{n-4}\). Now expanding \(S(n + d, n)\) into a degree \(d\) polynomial in \(n\)-odd via Lemma 1, we obtain by Proposition 9 and the formula (16)
\[ S(n + d, n) \equiv_2 n^d S(n, n) + \sum_{j=0}^{d-1} n^j S(n - 1 + (d - j), n - 1) \]
\[ \equiv_2 1 + \sum_{j=0}^{d/2} S(\ell_{n-4} + (d - 2j), \ell_{n-4}) \]
\[ + \sum_{j=0}^{d/2-1} S(n - 1 + (d - 2j - 1), n - 1). \]

Noting \(\ell_n > 4\), it follows \(4 \mid (n-1)\). Thus Proposition 8 implies \(2 \mid S(n-1+(d-2j-1), n-1)\) for each \(0 \leq j \leq d/2 - 1\). That is,
\[ \sum_{j=0}^{d/2-1} S(n - 1 + (d - 2j - 1), n - 1) \equiv_2 0. \]
Finally, since
\[ 1 \equiv_2 S(\ell_{n-4}, \ell_{n-4}) \]
the Proposition is established by taking (21) and (22) in (20). \(\square\)

**Remark 4.** We may now construct an infinite matrix which exhibits the distribution of the even and odd numbers \(S(n + d, n)\) if \(d \in \mathbb{N} \setminus \mathbb{O}\):
\[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & \ldots \\
1 & 0 & 1 & 0 & 1 & \ldots \\
1 & 1 & 0 & 0 & 1 & \ldots \\
1 & 0 & 0 & 1 & 1 & \ldots \\
1 & 1 & 1 & 1 & 0 & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{bmatrix}
\]
In matrix $P$, each entry $p_{ij}$ ($i, j \in \mathbb{N}$) denotes the parity of those numbers $S(n + d, n)$ ($d \in \mathbb{N} \setminus \mathbb{O}$) which satisfy $\ell_n = 1 + 4i = 1 + 4[(n - 1)/4]$ and $d = 2j$. The $p_{ij}$ are determined by the equations

$$p_{0j} = p_{i0} = 1 \quad (i, j \geq 0) \quad (23)$$

$$p_{ij} = \left( \sum_{k=0}^{j} p_{i-1,k} \right) \pmod{2} = (p_{i-1,j} + p_{i,j-1}) \pmod{2} \quad (i, j \geq 1) \quad (24).$$

(As an example, below we compute $P_{100} = [p_{ij} : 0 \leq i, j \leq 100]$ (Figure 6). This matrix is profitably represented as a "tapestry" of colored tiles, so that its interesting geometric properties are accentuated.)

![Figure 6. $P_{100}$. Above, yellow tiles correspond to $p_{ij} = 1$. Notice that this image is the Sierpinski Gasket.](image)

Although (24) is nothing more than a reformulation of Proposition 10, the second equality in (24) (from left to right) indicates that $P$ is Pascal (to visualize this, rotate $P$ $45^\circ$ so that $p_{00}$ is the "top" of Pascal’s Triangle modulo 2.) Thus, $P$ is symmetric, and an elementary geometric analysis yields

$$S(\ell_n + d, \ell_n) \equiv_2 \binom{i + j}{j} \equiv_2 \binom{i}{i} \quad (\ell_n = 1 + 4i, d = 2j). \quad (25)$$

Now, by Kummer’s Theorem, we have that

$$\binom{i + j}{j} \equiv_2 0 \text{ iff there exists } k \in \mathbb{N} \text{ such that } (i_2)_k = (j_2)_k = 1. \quad (26)$$

Hence the following is immediate:
Proposition 11. Let \( d \in \mathbb{E} \). Then \( 2 \mid S(m, n) \) if, and only if, there exists \( k \in \mathbb{N} \) such that
\[
\left( \binom{n - 1}{4} \right)_k = \left( \binom{d}{2} \right)_k = 1.
\]

Proof. By Proposition 9 and (25),
\[
S(m, n) \equiv_2 S(\ell_n + d, \ell_n) \equiv_2 \binom{i + j}{j} \quad (i = \lfloor (n - 1)/4 \rfloor, \ d = 2j).
\]
Hence the Proposition follows by (26). \( \square \)

Remark 5. Although Proposition 11 provides an elegant means to calculate the parity of \( S(m, n) \) if \( d \in \mathbb{E} \), it may be further improved. Notice that Proposition 10 implies the \( i^{th} \) row sequence
\[
R_i = (R_i(j))_{j \in \mathbb{N}} = (S(\ell_n + 2j, \ell_n) \ (\text{mod} \ 2))_{j \in \mathbb{N}} \quad (\ell_n = 1 + 4i)
\]
is periodic. Thus, by the symmetry of \( P \), the \( j^{th} \) column sequence
\[
C_j = (C_j(i))_{i \in \mathbb{N}} = (S(1 + 4i + d, 1 + 4i) \ (\text{mod} \ 2))_{i \in \mathbb{N}} \quad (d = 2j)
\]
is also periodic. Denote the periods of these sequences as \( T(R_i) \) and \( T(C_j) \), respectively. We remark that since \( P \) is Pascal, \( i = j \) implies \( R_i = C_j \). Conversely, \( i \neq j \) implies \( R_i \neq R_j \) and \( C_i \neq C_j \) (Proposition 13). We now show that both \( T(R_i) \) and \( T(C_i) \) are easily computed via (26).

Proposition 12. Let \( d \in \mathbb{E} \) and let \( \tau \) denote the MSB position of \( i_2 \neq 0 \). Then,
\[
T(R_\tau) = 2^{\tau + 1}.
\]

Proof. Notice that \( \tau \) is the MSB position of \( i_2 \) implies
\[
\{ k \in \mathbb{N} : (i_2)_k = (j_2)_k = 1 \} = \{ k \in \mathbb{N} : (i_2)_k = (j_2 + q2^{\tau + 1})_k = 1 \} \quad (q \in \mathbb{N}).
\]
Hence, (26) gives
\[
\binom{i + j}{j} \equiv_2 \binom{i + j + q2^{\tau + 1}}{j + q2^{\tau + 1}} \quad (q \in \mathbb{N}).
\]
Now by (27), we obtain \( T(R_\tau) \mid 2^{\tau + 1} \). Assume \( T(R_\tau) = 2^{\tau'} \) for some \( 0 \leq \tau' \leq \tau \). Noting \( p_{i_0} = 1 \), Kummer’s Theorem then assures \( (i_2)_k = 0 \) for \( \tau' < k \leq \tau \), for otherwise there exists \( t \in \mathbb{N} \) such that
\[
1 \equiv_2 \binom{i}{0} \equiv_2 \binom{i + 2^{\tau '+ t}}{2^{\tau '+ t}} \equiv_2 0.
\]
Thus \( (i_2)_\tau = 0 \), contradicting the hypothesis. This result furnishes \( T(R_\tau) \geq 2^{\tau + 1} \), and therefore \( T(R_\tau) = 2^{\tau + 1} \) holds. \( \square \)

Corollary 5. Let \( d \in \mathbb{E} \) and let \( \eta \) denote the MSB position of \( j_2 \neq 0 \). Then,
\[
T(C_\eta) = 2^{\eta + 1}.
\]

Proof. By the hypothesis and Proposition 12, we have that \( T(R_j) = 2^{\eta + 1} \). Hence, the symmetry of \( P \) yields \( T(C_j) = 2^{\eta + 1} \) as desired. \( \square \)
Remark 6. We may now improve (26) in the following sense. Given \( i \) and \( j \), consider \( p_{ij} \). Due to Proposition 12, one obtains an equal entry by replacing \( j \) with \( j' = j \pmod{T(R_i)} \). Similarly by Corollary 5, a replacement of \( i \) with \( i' = i \pmod{T(C_j)} \) also yields an equal entry. This process may be alternatively initiated with a replacement of \( i \) and ended with a replacement of \( j \) (depending upon which approach is most efficient, however observation of order is necessary). We make this reduction in computational work precise below.

Corollary 6. Let \( d \in \mathbb{E} \) such that \( d = 2j \), and \( \ell_n = 1 + 4i \). Denote
\[
 j^1 = j \pmod{T(R_i)}, \quad i^1 = i \pmod{T(C_j)}, \quad i^2 = i \pmod{T(C_j)}, \quad j^2 = j \pmod{T(R_i)}.
\]
Then, \( \nu_2(S(m, n)) \geq 1 \) if, and only if, there exists \( k \in \mathbb{N} \) such that
\[
 (A) \quad (i^1_k) = (j^1_k) = 1 \quad \text{and} \quad (i^2_k) = (j^2_k) = 1.
\]

Proof. The assertion follows by applying Proposition 12 and Corollary 5 to (26). □

Let \( i \in \mathbb{N} \) be given and \( \tau \) be as in Proposition 12. Call
\[
f_i = (R_i(0), R_i(1), \ldots, R_i(2^{r+1} - 1))
\]
the parity frequency of \( R_i \). It will now be shown that the parity frequency associated to each \( R_i \) is unique.

Proposition 13 (Uniqueness of Parity Frequencies). Let \( i, k \in \mathbb{N}, i \neq k \). Then, \( f_i \neq f_k \).

Proof. Assuming the hypothesis, suppose \( f_i = f_k \). Setting \( M = \max\{i, k\} \geq 1 \), consider the matrix \( P_M = [p_{ij} : 0 \leq i, j \leq M] \) (where \( p_{ij} \) is defined as in Remark 4). Since we have that \( M < T(R_M) \) (a consequence of Proposition 12), it follows by our assumption that rows \( i \) and \( k \) in \( P_M \) are identical. Hence \( \det(P_M) = 0 \). However \( P_M \) is Pascal, so that \( \det(P_M) \equiv 1 \pmod{2} \) (contradiction). Therefore, we conclude that \( f_i \neq f_k \). □

3. A Generalization of Wilson’s Theorem

We attribute the technique used in the proof below to Ruiz [2].

Proposition 14 (Generalized Wilson’s Theorem). Let \( p \in \mathbb{Z}_+ \). Then \( p \) is prime if, and only if, for every \( n \in \mathbb{Z}_+ \)
\[
-1 \equiv_p B(n(p - 1), p - 1).
\]

Proof. We first establish necessity. For the case \( p = 2 \), one observes that for every \( n \in \mathbb{Z}_+ \)
\[
B(n(p - 1), p - 1) \equiv 1 ! S(n, 1) \equiv 2 - 1.
\]

Now if \( p > 2 \) is prime, we have by Propositions 1 and 2 that
\[
(p - 1) ! S(n(p - 1), p - 1, 0) \equiv_p B(n(p - 1), p - 1).
\]

Expanding the LHS of (28) (recall the definition of \( S(m, n, z) \)), we obtain
\[
\sum_{k=0}^{p-1} \left( \begin{array}{c} p - 1 \\ k \end{array} \right) (-1)^k k^{n(p-1)} \equiv_p \sum_{k=0}^{p-1} \left( \begin{array}{c} p - 1 \\ k \end{array} \right) (-1)^k k^{p-1} \equiv_p B(n(p - 1), p - 1).
\]

Since
\[
\left( \begin{array}{c} p - 1 \\ 0 \end{array} \right) \equiv_p 1, \quad \left( \begin{array}{c} p - 1 \\ k \end{array} \right) + \left( \begin{array}{c} p - 1 \\ k - 1 \end{array} \right) \equiv_p \left( \begin{array}{c} p \\ k \end{array} \right) \equiv_p 0 \Rightarrow \left( \begin{array}{c} p - 1 \\ k \end{array} \right) \equiv_p -\left( \begin{array}{c} p - 1 \\ k - 1 \end{array} \right)
\]

it follows that for each $0 < k < p$,  
\[ \binom{p - 1}{k} \equiv_p (-1)^k. \]
Hence we have that  
\[ \sum_{k=0}^{p-1} \binom{p - 1}{k} (-1)^k \prod_{j=1}^{n} k^{p-1} \equiv_p \sum_{k=0}^{p-1} \prod_{j=1}^{n} k^{p-1}. \]
Finally, by Fermat’s Little Theorem, we conclude  
\[ \sum_{k=0}^{p-1} \prod_{j=1}^{n} k^{p-1} \equiv_p \sum_{k=0}^{p-1} \prod_{j=1}^{n} k^{p-1}. \]
For sufficiency, one observes that $-1 \equiv_p B(p - 1, p - 1)$ yields $-1 \equiv_p (p - 1)!$, which implies that $p$ is prime.

\textbf{Corollary 7 (Wilson’s Theorem).} Let $p \in \mathbb{Z}_+$. Then $p$ is prime if, and only if,  
\[ -1 \equiv_p (p - 1)! \pmod{p}. \]
\textbf{Proof.} If $p$ is prime, take $n = 1$ in Proposition 14 to obtain $-1 \equiv_p (p - 1)! \pmod{p}$.\hfill \Box

Proposition 14 may be applied to investigate the relationship between the Stirling numbers of the second kind and the primes. A result due to De Maio and Touset [4, Thm. 1 and Cor. 1] states that if $p > 2$ is prime, then  
\begin{equation}
S(p + n(p - 1), k) \equiv_p 0
\end{equation}
for every $n \in \mathbb{N}$ and $1 < k < p$. As an example of applying the Generalized Wilson’s Theorem, we have:

\textbf{Proposition 15.} Let $p > 2$ be prime. Then, for every $n \in \mathbb{Z}_+$ and $0 < k < p - 1$,  
\[ S(n(p - 1), p - k) \equiv_p (k - 1)!. \]
\textbf{Proof.} Appealing to Proposition 14, we have that for every $n \in \mathbb{Z}_+$  
\[ -1 \equiv_p (p - 1)!S(n(p - 1), p - 1) \equiv_p -S(n(p - 1), p - 1). \]
Hence $S(n(p - 1), p - 1) \equiv_p 1 \equiv_p (1 - 1)!$. Assume now that for $0 < \xi < p - 1$ we have  
\begin{equation}
S(n(p - 1), p - \xi) \equiv_p (\xi - 1)! \quad (n \in \mathbb{Z}_+).
\end{equation}
Let $n_0 \in \mathbb{Z}_+$ and $\xi + 1 < p - 1$. By (29) it follows  
\[ S(p + (n_0 - 1)(p - 1), p - \xi) \equiv_p S(n_0(p - 1) + 1, p - \xi) \]
\[ \equiv_p (p - \xi)S(n_0(p - 1), p - \xi) + S(n_0(p - 1), p - (\xi + 1)) \]
\[ \equiv_p -\xi S(n_0(p - 1), p - \xi) + S(n_0(p - 1), p - (\xi + 1)) \]
\begin{equation}
\equiv_p 0.
\end{equation}
Thus (30) and (31) imply that  
\[ S(n_0(p - 1), p - (\xi + 1)) \equiv_p \xi S(n_0(p - 1), p - \xi) \equiv_p \xi(\xi - 1)! \equiv_p \xi!. \]
Since $n_0$ is arbitrary, the Proposition follows by induction. \hfill \Box

\textbf{Acknowledgments.} This paper presents an undergraduate research project supported and supervised by Dr. Vladimir Dragovic at UT Dallas.
REFERENCES

[1] K. Boyadzhiev, *Close Encounters with the Stirling Numbers of the Second Kind*, Math. Mag. 85 (2012) 252-266. doi:10.4169/math.mag.85.4.252

[2] S. Ruiz, *An Algebraic Identity Leading to Wilson's Theorem*, The Math. Gazette 80 (1996) 579-582. http://dx.doi.org/10.2307/3618534

[3] H.W. Gould, *Combinatorial Numbers and Associated Identities*, published by West Virginia University, 2010. www.math.wvu.edu/~gould/Vol.7.PDF

[4] Joe De Maio, Stephen Touset, *Stirling Numbers of the Second Kind and Primality*, published by Kennesaw State University, 2008. http://science.kennesaw.edu/~jdemai/STIRLING%20SECOND%20PRIMES.pdf

[5] Alan Edelman, Gilbert Strang, *Pascal Matrices*, published by Department of Mathematics, Massachusetts Institute of Technology. http://web.mit.edu/18.06/www/Essays/pascal-work.pdf