A COMBINATORIAL IDENTITY INVOLVING ROOTS OF UNITY

DOW LAFEVERS

ABSTRACT. In this paper, we extend a commonly-encountered identity regarding the number of subsets of an $n$-set divisible by 2 to an arbitrary divisor; we first derive this identity algebraically to help explain why complex numbers (specifically roots of unity) appear in an identity involving only integers. This in turn motivates a combinatorial proof of this identity. We end by showing that the intuitive number of subsets of an $n$-set divisible by $k$ holds as $n$ tends to infinity.

CONTENTS

1. Introduction 1
2. Derivation of the Identity 2
3. Combinatorial Proof 3
4. Things are as they should be 6
Acknowledgments 7
References 8

1. Introduction

We read the binomial coefficient $\binom{n}{k}$ as “$n$ choose $k$”, alluding to the combinatorial interpretation of the symbol: it is the number of distinct ways of selecting a $k$-element subset from an $n$-element set. This inherent combinatorial structure often appears in so-called combinatorial proofs, where one counts the cardinality of some explicitly defined set two different ways to obtain two equivalent expressions for a given identity. As a method, the combinatorial proof may sometimes be more efficient than other methods, but the real upshot is that it provides insight into the underlying structure described by the identity.

Example 1.1. Finite sums of binomial coefficients are among the first identities encountered in a discrete math course. We recall that, for $n \geq 0$,

$$\sum_{k \geq 0} \binom{n}{k} = 2^n$$

and for $n \geq 1$,

$$\sum_{k \geq 0} \binom{n}{2k} = 2^{n-1}.$$
The sums are finite since $\binom{n}{k} = 0$ whenever $k > n$. Both identities have succinct algebraic explanations using the binomial theorem, but their combinatorial proofs are simultaneously more elegant and more insightful with respect to the structures which they enumerate. Beautiful combinatorial proofs of both identities can be found in [2] as Identities 128 and 129.

2. Derivation of the Identity

Having seen the two identities in Example 1.1 we may reasonably expect that, for $r \geq 3$, the sum

$$\sum_{k \geq 0} \binom{n}{rk}$$

is similarly easy to evaluate to obtain a simple closed form. However, for $r \geq 3$, the closed form of (2.1) is harder to derive and notably more complex.

Theorem 2.2. For $n \geq 0$ and $r \geq 1$,

$$\sum_{k \geq 0} \binom{n}{rk} = \frac{1}{r} \sum_{j=0}^{r-1} (1 + \omega^j)^n,$$

where $\omega = e^{\frac{2\pi i}{r}}$ is a primitive $r$th root of unity.

Remark 2.4. A beautiful identity, no doubt, but if you’re anything like the author of this paper, you are—if not deeply troubled and visibly agitated, at the very least—somewhat disappointed. For if the number of subsets of an $n$-set is $2^n$, and the number of subsets with cardinality divisible by 2 is $2^n/2 = 2^{n-1}$, morally speaking, it seems it ought to be the case that the number of subsets of an $n$-set with cardinality divisible by $r$ is $2^n/r$... Worry not! In Section 4, we will show that things are how they should be; that is, we will show that $\sum_{k \geq 0} \binom{n}{rk}$ is asymptotically equivalent to $2^n/r$ as $n \to \infty$.

There exist at least 4 different ways to prove Theorem 2.2. In this paper, we present two proofs that provide insight into the underlying structure of the identity. We first prove the identity algebraically by way of the binomial theorem, a proof which helps to explain the otherwise unexpected appearance of complex numbers in what one would expect to be an integer identity. We notice that, by taking advantage of the unique properties of roots of unity, we are able to explicitly define an indicator function that causes the binomial coefficients without cardinality divisible by $r$ to vanish while also assigning unit weight to the coefficients we wish to preserve. Fortunately, it turns out that this function is, in addition, easy to sum.

Proof. In order to put (2.1) in a more palatable form, we first explicitly define an indicator function: for $r \geq 1$ and $k \geq 0$, define

$$1_k = \frac{1}{r} \sum_{j=0}^{r-1} \omega^{kj}$$

where $\omega = e^{\frac{2\pi i}{r}}$ is a primitive $r$th root of unity. We claim that

$$1_k = \begin{cases} 1 & \text{if } r \mid k \\ 0 & \text{if } r \nmid k. \end{cases}$$

There exist at least 4 different ways to prove Theorem 2.2. In this paper, we present two proofs that provide insight into the underlying structure of the identity. We first prove the identity algebraically by way of the binomial theorem, a proof which helps to explain the otherwise unexpected appearance of complex numbers in what one would expect to be an integer identity. We notice that, by taking advantage of the unique properties of roots of unity, we are able to explicitly define an indicator function that causes the binomial coefficients without cardinality divisible by $r$ to vanish while also assigning unit weight to the coefficients we wish to preserve. Fortunately, it turns out that this function is, in addition, easy to sum.
For proof, notice that if $r \mid k$, then $\omega^k = 1$. Hence

$$1_k = \frac{1}{r} \sum_{j=0}^{r-1} (\omega^k)^j = \frac{1}{r} \sum_{j=0}^{r-1} 1 = 1.$$  

Alternatively, if $r \nmid k$, then $\omega^k \neq 1$. Recalling the formula for the partial sums of a geometric series, we obtain

$$1_k = \frac{1}{r} \sum_{j=0}^{r-1} (\omega^k)^j = \frac{1}{r} \frac{1 - \omega^k}{1 - \omega} = 0$$

as promised.

We can now substitute this indicator function into (2.1):

$$\sum_{k \geq 0} \binom{n}{rk} = \sum_{k=0}^{n} \binom{n}{k} 1_k = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{r} \sum_{j=0}^{r-1} \omega^{kj}.$$  

Our gut reaction, to interchange the sums, turns out to be quite effective, as doing so allows us to apply the binomial theorem (an elegant combinatorial proof of which appears as Identity 133 in [2]). Doing so, one obtains

$$\sum_{k=0}^{n} \binom{n}{k} \frac{1}{r} \sum_{j=0}^{r-1} \omega^{kj} = \frac{1}{r} \sum_{j=0}^{r-1} (1 + \omega^j)^n.$$  

Thus, we have

$$\sum_{k \geq 0} \binom{n}{rk} = \frac{1}{r} \sum_{j=0}^{r-1} (1 + \omega^j)^n$$

as desired. □

### 3. Combinatorial Proof

Having confirmed that Theorem 2.2 is indeed true, we now introduce a few definitions towards a combinatorial proof of the identity, modelled after that given by Arthur et al. in [1].

**Definition 3.1.** Our proof will utilize $C_r$, the directed, looped cycle graph with vertex set $V = \{0, 1, \ldots, r-1\}$ such that for each $j \in V$, there exists an edge from $j$ to $j + 1$ (mod $r$). (See Figure 1.)

**Definition 3.2.** An $n$-walk is a walk on $C_r$ that takes exactly $n$ steps. We say such a walk is closed if it begins and ends at the same vertex. Otherwise, we say the walk is open. Moreover, we define a forward step as an arc from vertex $j$ to vertex $j + 1$ (mod $r$) and a stationary step as an arc from vertex $j$ to itself.

Observe that an $n$-walk starting at $x_0$ and making $m$ forward steps ends up at vertex $x_0 + m$ (mod $r$). Consequently, an $n$-walk is closed if and only if $m \equiv 0$ mod $r$.

**Definition 3.3.** Let $X_0$ be an open walk which takes $m \not\equiv 0$ (mod $r$) forward steps with initial vertex $x_0 = 0$. Then the orbit of $X_0$ is the collection $\{X_0, X_1, \ldots, X_{r-1}\}$ such that $X_j$ starts at vertex $j$ and follows the same sequence of forward and stationary steps as $X_0$ to end up at vertex $j + m$ (mod $r$).
We are now equipped to prove Theorem 2.2 by way of a double-counting argument.

**Proof.** Let $S$ denote the set of closed $n$-walks on $C_r$. We count the elements of $S$ two ways. First, we notice that for $0 \leq m \leq n$, there are $\binom{n}{m}$ $n$-walks that take $m$ forward steps. Since a walk is closed if and only if $m \equiv 0 \mod r$, a walk with $m$ forward steps is closed if and only if $m$ is a multiple of $r$. Hence,

$$|S| = \sum_{k \geq 0} \binom{n}{r^k}.$$  

Alternatively, we can count the number of closed $n$-walks on $C_r$ by assigning a weight to each walk. Observing that the number of closed $n$-walks beginning at vertex 0 is the same as those starting at vertex 1 or 2 or... or $r-1$, it will suffice to show that the total number of closed $n$-walks on $C_r$ is $\sum_{j=0}^{r-1} (1 + \omega^j)^n$ with the proviso that we will ultimately divide by $r$ to count only those closed walks beginning at vertex 0, thereby recovering our identity. We assign a weight to each $n$-walk on $C_r$ depending on its initial vertex and its number of forward moves. Specifically, for a walk with initial vertex $j$ which takes $m$ forward steps, we assign weight $\omega^j m$. In particular, we notice that any closed walk has weight 1 since $m \equiv 0 \mod r$ implies $\omega^j m = \omega^{jk} = (\omega^r)^j k = 1$ for some $k$.

Equivalently, we can think of the weight of a walk with $x_0 = j$ as assigning weight 1 to a stationary step and weight $\omega^j$ to a forward step, where the total weight of the walk is then defined as the product of the weights of its steps. Since any $n$-walk on $C_r$ is composed of $n$ such decisions (either 1 or $\omega^j$), it follows that the total weight of all $n$-walks with $x_0 = j$ is $(1 + \omega^j)^n$. This decision-type argument corresponds with the combinatorial interpretation of $(1 + \omega^j)^n$ given by the binomial theorem: $(1 + \omega^j)^n = \sum_{k \geq 0} \binom{n}{k} \omega^{jk}$ is the sum of the total weight of all $n$-walks on $C_r$ with

**Figure 1.** $C_5$, the looped cycle graph on 5 vertices [1]
A combinatorial identity involving roots of unity

Let \( x_0 = j \) since \( \binom{n}{k} \omega^{jk} \) is the total weight of all \( n \)-walks with \( x_0 = j \) that take \( k \) forward steps. Summing across all possible starting points, the total weight of all \( n \)-walks on \( C_r \) is therefore given by

\[
(3.4) \quad \sum_{j=0}^{r-1} (1 + \omega^j)^n.
\]

We claim that (3.4) counts the total number of closed walks on \( C_r \). Since each closed walk has unit weight, it is sufficient to show that the total weight of all open walks is 0. To do so, we recall the notion of an orbit as defined in Definition 3.3. Take an arbitrary open walk beginning at vertex 0 that takes \( m \) forward steps. Then the weight of each \( n \)-walk in the orbit generated by this walk is given by \( \omega^{jm} \) for \( 1 \leq j \leq r-1 \), which implies the total weight of all \( n \)-walks in this orbit is given by

\[
\frac{1}{r} \sum_{j=0}^{r-1} \omega^{jm} = \frac{1 - \omega^m}{1 - \omega} = 0,
\]

since \( \omega^m = 1 \) and \( \omega^m \neq 1 \). Since the total weight of each orbit is 0 and each open walk appears in precisely one orbit, the total weight of all open walks is zero, as promised. Hence (3.4) counts only the closed \( n \)-walks on \( C_r \). Since the number of closed \( n \)-walks beginning at any vertex is the same, the number of closed walks beginning at vertex 0 is

\[
\frac{1}{r} \sum_{j=0}^{r-1} (1 + \omega^j)^n = |S|
\]

as desired. \( \square \)

It’s interesting to note that this method, sometimes referred to as “weighted enumeration,” generalizes readily by slightly changing the weight function. The author initially discovered Theorem 2.2 by working out the case of \( r = 3 \) and noticing that it generalizes immediately. Similarly, the case of \( r = 7 \) appears in [5] as Exercise 1.42(f), and the proof given in the solutions is done in almost full generality. It turns out that the natural generalization of Theorem 2.2, which appears in [4] as Identity 1.53, follows using the same machinery as the simpler case:

**Theorem 3.5.** For \( 0 \leq a < r \) and \( n \geq 0 \),

\[
\sum_{k \geq 0} \binom{n}{a + rk} = \frac{1}{r} \sum_{j=0}^{r-1} \omega^{-ja} (1 + \omega^j)^n
\]

where \( \omega = e^{2\pi i / r} \) is a primitive \( r \)th root of unity.

**Proof.** We count the same quantity, where a closed walk is defined as a walk where \( m = a + rk \) where \( m \) is the number of forward steps and \( k \) is some nonnegative integer. As is clear from the first part of the combinatorial proof of Theorem 2.2, this quantity is counted by \( \sum_{k \geq 0} \binom{n}{a+rk} \).

To count this quantity a different way, we adjust our weighting scheme so that an \( n \)-walk on \( C_r \) that starts at vertex \( j \) and takes \( m \) forward steps has weight \( \omega^{(m-a)j} = \omega^m \omega^{-ja} \). Thus, any walk which takes \( a + rk \) forward steps has weight \( x_0 = j \) since \( \binom{n}{k} \omega^{jk} \) is the total weight of all \( n \)-walks with \( x_0 = j \) that take \( k \) forward steps. Summing across all possible starting points, the total weight of all \( n \)-walks on \( C_r \) is therefore given by

\[
\sum_{j=0}^{r-1} (1 + \omega^j)^n.
\]

We claim that (3.4) counts the total number of closed walks on \( C_r \). Since each closed walk has unit weight, it is sufficient to show that the total weight of all open walks is 0. To do so, we recall the notion of an orbit as defined in Definition 3.3. Take an arbitrary open walk beginning at vertex 0 that takes \( m \) forward steps. Then the weight of each \( n \)-walk in the orbit generated by this walk is given by \( \omega^{jm} \) for \( 1 \leq j \leq r-1 \), which implies the total weight of all \( n \)-walks in this orbit is given by

\[
\frac{1}{r} \sum_{j=0}^{r-1} \omega^{jm} = \frac{1 - \omega^m}{1 - \omega} = 0,
\]

since \( \omega^m = 1 \) and \( \omega^m \neq 1 \). Since the total weight of each orbit is 0 and each open walk appears in precisely one orbit, the total weight of all open walks is zero, as promised. Hence (3.4) counts only the closed \( n \)-walks on \( C_r \). Since the number of closed \( n \)-walks beginning at any vertex is the same, the number of closed walks beginning at vertex 0 is

\[
\frac{1}{r} \sum_{j=0}^{r-1} (1 + \omega^j)^n = |S|
\]

as desired. \( \square \)

It’s interesting to note that this method, sometimes referred to as “weighted enumeration,” generalizes readily by slightly changing the weight function. The author initially discovered Theorem 2.2 by working out the case of \( r = 3 \) and noticing that it generalizes immediately. Similarly, the case of \( r = 7 \) appears in [5] as Exercise 1.42(f), and the proof given in the solutions is done in almost full generality. It turns out that the natural generalization of Theorem 2.2, which appears in [4] as Identity 1.53, follows using the same machinery as the simpler case:

**Theorem 3.5.** For \( 0 \leq a < r \) and \( n \geq 0 \),

\[
\sum_{k \geq 0} \binom{n}{a + rk} = \frac{1}{r} \sum_{j=0}^{r-1} \omega^{-ja} (1 + \omega^j)^n
\]

where \( \omega = e^{2\pi i / r} \) is a primitive \( r \)th root of unity.

**Proof.** We count the same quantity, where a closed walk is defined as a walk where \( m = a + rk \) where \( m \) is the number of forward steps and \( k \) is some nonnegative integer. As is clear from the first part of the combinatorial proof of Theorem 2.2, this quantity is counted by \( \sum_{k \geq 0} \binom{n}{a+rk} \).

To count this quantity a different way, we adjust our weighting scheme so that an \( n \)-walk on \( C_r \) that starts at vertex \( j \) and takes \( m \) forward steps has weight \( \omega^{(m-a)j} = \omega^m \omega^{-ja} \). Thus, any walk which takes \( a + rk \) forward steps has weight
\[ \omega^{rkj} = 1. \]

By the same argument given in the combinatorial proof of Theorem 2.2, the total weight of all \( n \)-walks on \( C_r \) is

\[ \sum_{j=0}^{r-1} \omega^{-ja}(1 + \omega^j)^n. \]

Then the theorem follows by noticing that walks where \( m \neq a + rk \) (i.e. open walks) can be put into orbits with vanishing weight; that is, with total weight

\[ \sum_{j=0}^{r-1} \omega^{(m-a)j} = \frac{1-\omega^{(m-a)r}}{1-\omega^{r}} = 0. \]

Hence, the number of closed walks beginning at vertex 0 is given by

\[ \frac{1}{r} \sum_{j=0}^{r-1} \omega^{-ja}(1 + \omega^j)^n \]

as desired. \( \Box \)

4. Things are as they should be

We now make good on our promise from Remark 2.4. We use the definition of asymptotic equivalence given in [3]:

**Definition 4.1.** Given functions \( f(x) \) and \( g(x) \) with a shared domain, we define a binary relation

\[ f(x) \sim g(x) \quad \text{(as } x \to \infty) \]

if and only if

\[ \lim_{x \to \infty} \frac{f(x)}{g(x)} = 1. \]

When \( f(x) \sim g(x) \), we say the functions \( f \) and \( g \) are asymptotically equivalent.

**Corollary 4.2.** For fixed \( r \geq 1 \),

\[ \sum_{k \geq 0} \binom{n}{rk} \sim \frac{2^n}{r} \quad \text{as } n \to \infty. \]

We first endeavor to make our expression entirely real.

**Proposition 4.3.** For \( n \geq 0 \) and \( r \geq 1 \),

\[ \sum_{k \geq 0} \binom{n}{rk} = \frac{2^n}{r} + \frac{2^{n+1}}{r} \cos \frac{\pi j}{r} \cos \frac{n\pi j}{r} \]

where \( \omega = e^{2\pi i/r} \) is a primitive \( r \)-th root of unity and \( \lfloor x \rfloor \) takes the integer part of a real number \( x \).

**Proof.** From Theorem 2.2, we have

\[ \sum_{k \geq 0} \binom{n}{rk} = \frac{1}{r} \sum_{j=0}^{r-1} (1 + \omega^j)^n. \]

Noticing that \( \omega^{r-j} = \omega^{-j} \), we can rewrite the right hand side as

\[ \frac{2^n}{r} + \frac{1}{r} \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} [(1 + \omega^j)^n + (1 + \omega^{-j})^n]. \]

Here, we have pulled out the \( j = 0 \) term, combined the \( j \) and \( r-j \) terms, and used the fact that if \( r \) is even and \( j = r/2, 1 + \omega^j = 1 + e^{i\pi} = 0 \) (Euler’s identity). We now recognize that \( (1 + \omega^j)^n \) and \( (1 + \omega^{-j})^n \) are complex conjugates, which means we can replace their sum by twice their real part to obtain

\[ \frac{2^n}{r} + \frac{1}{r} \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} 2 \cdot \Re [(1 + \omega^j)^n]. \]

(4.4)
We now turn our attention to putting the $1 + \omega^j$ term into a more workable form by way of the familiar double angle formulae and Euler’s formula:

$$1 + \omega^j = 1 + \cos \frac{2\pi j}{r} + i \sin \frac{2\pi j}{r} \quad \text{Euler’s formula}$$

$$= 2 \cos^2 \frac{\pi j}{r} + 2i \sin \frac{\pi j}{r} \cos \frac{\pi j}{r} \quad \text{double-angle formulae}$$

$$= 2 \cos \frac{\pi j}{r} \left( \cos \frac{\pi j}{r} + i \sin \frac{\pi j}{r} \right).$$

Thus, we can write

$$(1 + \omega^j)^n = \left( 2 \cos \frac{\pi j}{r} \left[ \cos \frac{\pi j}{r} + i \sin \frac{\pi j}{r} \right] \right)^n = 2^n \cos^n \frac{\pi j}{r} \left[ \cos \frac{n\pi j}{r} + i \sin \frac{n\pi j}{r} \right]$$

by applying De Moivre’s formula. Returning to (4.4), we have

$$\frac{2^n}{r} + \frac{1}{r} \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} 2 \Re \left[(1 + \omega^j)^n\right] = \frac{2^n}{r} + \frac{2^{n+1}}{r} \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} \cos^n \frac{\pi j}{r} \cos \frac{n\pi j}{r}$$

as desired. \[\square\]

We are now prepared to prove Corollary 4.2.

**Proof.** Applying Proposition 4.3, we have

$$\lim_{n \to \infty} \sum_{k \geq 0} \binom{n}{rk} \frac{2^n}{r} = \lim_{n \to \infty} \frac{2^n}{r} + \frac{2^{n+1}}{r} \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} \cos^n \frac{\pi j}{r} \cos \frac{n\pi j}{r}$$

$$= \lim_{n \to \infty} 1 + 2 \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} \cos^n \frac{\pi j}{r} \cos \frac{n\pi j}{r}$$

$$= 1 + 2 \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} \lim_{n \to \infty} \cos^n \frac{\pi j}{r} \cos \frac{n\pi j}{r}.$$

Notice that $\lim_{n \to \infty} \cos^n \frac{\pi j}{r} = 0$ since $0 < j/r < 1$ for all $j$. Moreover, since $|\cos \frac{n\pi j}{r}| \leq 1$ for all $n$, we have $\lim_{n \to \infty} \cos^n \frac{\pi j}{r} \cos \frac{n\pi j}{r} = 0$. Hence,

$$\lim_{n \to \infty} \sum_{k \geq 0} \binom{n}{rk} \frac{2^n}{r} = 1 + 2 \sum_{j=1}^{\lfloor \frac{r-1}{2} \rfloor} \lim_{n \to \infty} \cos^n \frac{\pi j}{r} \cos \frac{n\pi j}{r} = 1 + 0 = 1,$$

which implies

$$\sum_{k \geq 0} \binom{n}{rk} \sim \frac{2^n}{r} \quad \text{as } n \to \infty.$$
ACKNOWLEDGMENTS

It is my pleasure to thank Charley Devlin for his crucial support throughout the whole summer, Daniil Rudenko for his insightful lectures, Polina Baron for running useful problem-sessions, and Peter May for his steadfast commitment to developing the next generation of mathematicians. I thank the Big Bang for everything else.
I would like to remind Zach Cogan that he owes me one (1) dollar.
Finally, I express my sincere gratitude to my parents for supporting me financially and with their love.

REFERENCES