Simple Formulas for Univariate Multinomial Coefficients

Joseph M. Shunia

September 2023
(Revised: July 2024, Version 7)

Abstract

We present novel arithmetic terms for univariate multinomial coefficients and their partial sums. Notably, we introduce what appear to be the first closed form expressions for partial sums of binomial coefficients. These results stem from an underutilized property of polynomials, which allows for their complete determination using only two evaluations under specific conditions. Applying our techniques to central trinomial coefficients, we resolve an open problem posed by Graham et al., demonstrating that no restricted class of "simple closed forms" can exclude these coefficients.

Keywords: elementary formula; arithmetic term; modular arithmetic; multinomial coefficient; binomial coefficient; partial sum; polynomial interpolation; Kronecker substitution.

2020 Mathematics Subject Classification: 11B65, 11Y55, 11A25.

1 Introduction

This paper marks the beginning of our exploration into the study of explicit arithmetic terms for integer sequences and number theoretic functions. We introduce the first known arithmetic terms for univariate multinomial coefficients and their partial sums. Remarkably, we also present what are possibly the only closed form expressions of any kind for the partial sums of binomial coefficients, as detailed in § 3. These foundational results help set the stage for further research into the study of arithmetic terms.

To fully appreciate the implications of these contributions, it is essential to understand what constitutes an arithmetic term. An arithmetic term is an integer-valued function that uses only the elementary arithmetic operations:

$$\{a + b, a \dot{-} b, ab, \lfloor a/b \rfloor, a \bmod b, a^b\},$$

where the notation $\dot{-}$ represents "truncated" or "bounded" subtraction, defined as $a \dot{-} b = \max(a - b, 0)$ [20, 16]. In this paper, we may use $-$ in place of $\dot{-}$ when it is clear that $(a - b) \geq 0$. We further note that the modulo operation is implicitly included in the set, as it can be defined by the others as: $a \bmod b = a \dot{-} b \lfloor a/b \rfloor$.

The study of arithmetic terms has its origins in the earliest days of computer science and discrete mathematics, tracing back to the 1950s and the work of Julia Robinson [8]. During that era, research primarily focused on broad theoretical questions about the capabilities of arithmetic terms in computability and their classification within mathematical logic [5, 2, 8]. In particular, a significant question was: What is the class of functions that can be represented using only these elementary arithmetic operations?

Mazzanti's 2002 discovery that arithmetic terms generate the class of Kalmar functions, denoted **K**, clarified their position in the Grzegorczyk hierarchy, a framework categorizing primitive recursive functions by complexity [20, 2]. In particular, Mazzanti's result placed arithmetic terms in the class $\mathcal{E}^3$ within the Grzegorczyk hierarchy, which is well-known to be equal to **K**. Further refinement by Marchenkov in 2006 demonstrated that even a more restricted set of functions could generate **K** [21]. Collectively, the works of Mazzanti-Marchenkov provide a strong theoretical underpinning for the study of arithmetic terms.

Despite these theoretical milestones, little attention has been given to the explicit construction and study of arithmetic terms until recently. Our research began in early 2022 with the dissemination of an early version of this paper. At around the same time, researchers Prunescu and Sauras-Altuzarra began their own independent investigations [13, 16].

Interestingly, functions that seem computationally simple, like the logarithm function $\log(n)$ or Hamming weight $\#(n)$ (the number of ones in the binary expansion of n), often lack straightforward arithmetic terms. Conversely, more complicated functions can sometimes be represented simply. Consider Robinson's elegant formula for the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ [8]:

$$\binom{n}{k} = \left\lfloor \frac{(2^n + 1)^n}{2^{nk}} \right\rfloor \bmod 2^n.$$

This asymmetry is an inversion of our expectations: One reasonably expects that sequences which are hard to compute should necessitate formulas that are sophisticated and hard to find, whereas sequences which are easy to compute should have formulas that are simple and easy to find.

Indeed, deriving arithmetic terms for many Kalmar functions has proven to be exceedingly challenging. Matiyasevich's work [24], for instance, confirms the existence of arithmetic terms for many prominent number theoretic functions that remain elusive, such as: The n-th prime number, the prime counting function, and Euler's totient function. Our hope is that the discovery and study of such formulas can yield new insights in number theory and other branches of mathematics.

1.1 Structure of the Paper

We begin in § 2 by proving a theorem stating that under certain conditions, a polynomial can be completely determined by only two evaluations (Theorem 2.1). This property allows us to recover the coefficients of a polynomial using an arithmetic term. Subsequently, we revisit an unconventional formula for binomial coefficients, initially given by Julia Robinson [8], and prove it as a corollary.

In § 3, we present arithmetic terms for the partial sums of binomial coefficients, for which it has been alleged that no explicit closed form expression is known [11, 23]. A formula we prove is

$$\sum_{k=0}^{j} \binom{n}{k} = \left\lfloor \frac{(2^n + 1)^n}{2^{n(n-j)}} \right\rfloor \bmod (2^n - 1).$$

We proceed in § 4 by generalizing Robinson's binomial coefficient formula to calculate the coefficients in the multinomial expansion of univariate unit polynomials. A univariate unit polynomial is a polynomial of the form

$$\left(\frac{x^r - 1}{x - 1} \right)^n = (x^{r-1} + \cdots + x + 1)^n,$$

and its multinomial expansion is given by

$$[x^k](x^{r-1} + \cdots + x + 1)^n.$$

The coefficients in the multinomial expansion of univariate unit polynomials are the univariate multinomial coefficients denoted as $\binom{n}{k}_{r-1}$, which are a generalization of the binomial coefficients. Conventional techniques for computing univariate multinomial coefficients involve factorials and summations over specific criteria. In contrast, our formula uses only elementary arithmetic operations and is given by

$$\binom{n}{k}_{r-1} = \left\lfloor \left(\frac{r^{rn} - 1}{r^{n+k} - r^k} \right)^n \right\rfloor \bmod r^n,$$

where $n > 0$ and $0 \le k \le n(r-1)$ (Theorem 4.1).

In § 5, we apply our multinomial coefficient formula to address an open problem posed by Graham et al. in their 1994 book *Concrete Mathematics: A Foundation for Computer Science* [18]. The problem concerns the existence of a restricted class of "simple closed forms" that excludes the sequence of central trinomial coefficients (A002426 in the OEIS). We present an argument suggesting a negative resolution to this question.

2 Polynomial Interpolation with Two Evaluations

We begin by presenting a theorem which shows how to recover a polynomial in $\mathbb{Z}[x]$ completely using only two carefully chosen evaluation points.

Theorem 2.1. *Given three non-negative integers $b > 0$, k, $r \ge k$, and a non-constant polynomial $f(x)$ of non-negative integer coefficients, degree r, such that $f(b) \ne 0$, we have that*

$$[x^k]f(x) = \left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b).$$

Proof. To prove the validity of the formula, we proceed by examining its arithmetic operations step-by-step.

Suppose we choose some k in the interval $[0, r]$. Now, let's consider the expansion of $f(f(b))$, which can be written as

$$f(f(b)) = a_r f(b)^r + a_{r-1} f(b)^{r-1} + \cdots + a_k f(b)^k + a_{k-1} f(b)^{k-1} + \cdots + a_1 f(b) + a_0,$$

where the a_i are coefficients in $\mathbb{Z}^+$.

The first step in the formula is to divide $f(f(b))$ by $f(b)^k$. This results in the quotient

$$\frac{f(f(b))}{f(b)^k} = f(b)^{-k}(a_r f(b)^r + \cdots + a_k f(b)^k + a_{k-1} f(b)^{k-1} + \cdots + a_0)$$

$$= a_r f(b)^r f(b)^{-k} + \cdots + a_k f(b)^k f(b)^{-k} + a_{k-1} f(b)^{k-1} f(b)^{-k} + \cdots + a_0 f(b)^{-k}$$

$$= a_r f(b)^{r-k} + \cdots + a_k f(b)^{k-k} + a_{k-1} f(b)^{k-k-1} + \cdots + a_0 f(b)^{-k}$$

$$= a_r f(b)^{r-k} + \cdots + a_k f(b)^0 + a_{k-1} f(b)^{-1} + \cdots + a_0 f(b)^{-k}$$

$$= a_r f(b)^{r-k} + \cdots + a_k + a_{k-1} f(b)^{-1} + \cdots + a_0 f(b)^{-k}.$$

Since $b \geq 1$, we have $f(b) \geq f(1)$. Thus, the coefficients of $a_{k-1} f(b)^{-1} + \cdots + a_0 f(b)^{-k}$ will sum to a value that is less than 1. The next step is to take the floor of the quotient $\frac{f(f(b))}{f(b)^k}$ to isolate the terms ranging from $a_k x^k$ up to and including $a_r x^r$. The result is

$$\left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor = a_r f(b)^{r-k} + \cdots + a_k.$$

The final step is to take the floored result $\left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor$ modulo $f(b)$. Carrying it out, we see

$$\left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b) = (a_r f(b)^{r-k} \bmod f(b)) + \cdots + (a_k \bmod f(b))$$

$$= 0 + \cdots + 0 + (a_k \bmod f(b))$$

$$= a_k \bmod f(b).$$

By assumption, all coefficients of $f(x)$ are non-negative. Furthermore, since $f(b) \geq f(1)$ and $\deg(f(x)) = r \geq 1$, we know that $f(b) > a_k$. Therefore, the modular reduction by $f(b)$ leaves the coefficient a_k unchanged. Thus, we arrive at

$$a_k = \left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b),$$

which is the formula we wanted to prove. $\square$

In proving Theorem 2.1, we have shown that, under the given conditions, it is possible to recover all the coefficients of $f(x)$ using only the values $f(b)$ and $f(f(b))$. Since we can recover the coefficient a_k from its degree k, we can determine the degree of the term corresponding to the coefficient recovered. Hence, we can reconstruct the polynomial $f(x)$ completely, with the correct degrees and coefficients for all of its terms.

Remark 2.1. *The polynomial property described in Theorem 2.1 appears to be underexplored in the literature. However, it has been the subject of some online discussions [15, 19] and at least one blog post [7]. Despite these mentions, the property has been treated mostly as a novelty or curiosity, and its applications have not been thoroughly examined.*

2.1 Binomial Coefficients

To provide an intuitive example of how Theorem 2.1 can be used, we provide a new proof of Robinson's binomial coefficient formula [8] as a corollary.

Corollary 2.1. *Let $n, k \in \mathbb{Z} : 0 \leq k \leq n$. Then*

$$\binom{n}{k} = \left\lfloor \frac{(2^n + 1)^n}{2^{nk}} \right\rfloor \bmod 2^n.$$

Proof. Consider the polynomial $f(x) := (x + 1)^n \in \mathbb{Z}[x]$. The binomial theorem gives the polynomial expansion

$$f(x) = (x + 1)^n = \sum_{j=0}^{n} \binom{n}{j} x^j 1^{n-j} = \sum_{j=0}^{n} \binom{n}{j} x^j.$$

By expanding out the inner terms of sum, we can see

$$f(x) = \binom{n}{0} x^0 + \binom{n}{1} x^1 + \cdots + \binom{n}{n-1} x^{n-1} + \binom{n}{n} x^n.$$

Hence, $f(x)$ is a polynomial with integer coefficients that are the binomial coefficients for row n of Pascal's triangle.

If we evaluate at $x = 1$, we get the coefficient sum. Applying this to $f(x)$, the evaluation $f(1)$ is equal to the sum of the coefficients of the n-th row of Pascal's triangle. This sum is well-known to be equal to 2^n [6]. Carrying out the evaluation, we get

$$f(1) = \binom{n}{0}1^0 + \binom{n}{1}1^1 + \cdots + \binom{n}{n-1}1^{n-1} + \binom{n}{n}1^n$$
$$= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n}$$
$$= 2^n.$$

Let $b = 1$, so that $f(b) = f(1) = 2^n$. By Theorem 2.1, for all $0 \le k \le n$, we can recover the coefficient $\binom{n}{k}$ using only the evaluations $f(b)$ and $f(f(b))$ by way of the formula

$$a_k = \left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b).$$

In this case, $a_k = \binom{n}{k}$. Substituting $f(b) = 2^n$ and $a_k = \binom{n}{k}$ into the formula, we get

$$\binom{n}{k} = \left\lfloor \frac{f(2^n)}{(2^n)^k} \right\rfloor \bmod 2^n.$$

Finally, by expanding $f(2^n) = (2^n + 1)^n$ and simplifying, we arrive at

$$\binom{n}{k} = \left\lfloor \frac{(2^n + 1)^n}{2^{nk}} \right\rfloor \bmod 2^n,$$

proving the formula. $\qquad\square$

2.2 Kronecker Substitution

The polynomial interpolation procedure described by Theorem 2.1 is closely related to the process of Kronecker substitution, which is a technique for encoding a polynomial as an integer [9].

Given a polynomial $f(x) \in \mathbb{Z}[x]$ and a suitable integer $b \in \mathbb{Z}$, Kronecker substitution evaluates $f(x)$ at $x = b$. By choosing an appropriate base b, the resulting integer $f(b)$ encodes the coefficients of f in its digits. An integer base b is said to be "suitable" for a polynomial f if b is greater than the sum of the absolute values of the coefficients of the polynomial, ensuring that the coefficients can be uniquely determined from the digits of $f(b)$. This technique is commonly used for fast polynomial multiplication [3, 4, 14, 10, 1]. However, its potential applications in number theory remain largely unexplored. The aim of this paper, along with our ongoing research, is to investigate and broaden the traditional applications of Kronecker substitution and related methods.

3 Partial Sums of Binomial Coefficients

Boardman (2004) asserted that "it is well-known that there is no closed form (that is, direct formula) for the partial sum of binomial coefficients" [11]. This statement has been cited in the Wikipedia article on binomial coefficients to suggest the impossibility of a closed form expression for these partial sums [23]. However, this interpretation appears to misconstrue Boardman's intended meaning. In his paper, Boardman references a theorem by Petkovšek et al. which proves the non-existence of a closed form expression for the partial sums of binomial coefficients specifically as a hypergeometric closed form [12]. In our opinion, it is more likely that Boardman was citing this result to indicate the absence of a known formula, rather than asserting the impossibility of any such formula. If indeed no closed form expression has been previously established, then the formulas we present here may constitute the first of their kind.

Theorem 3.1. *Let $n, j \in \mathbb{Z}_{>-1}$ such that $j \le n$. Then the following formulas are valid:*

(i)

$$\sum_{k=0}^{j} \binom{n}{k} = \left\lfloor \frac{(2^n + 1)^n}{2^{n(n-j)}} \right\rfloor \bmod (2^n - 1).$$

(ii)

$$\sum_{k=0}^{j} \binom{n}{k} = \left((2^n + 1)^n \bmod 2^{nj+1} \right) \bmod (2^n - 1).$$

Proof. The first step in formula (i) is to perform floored division on the sum $(2^n + 1)^n = \sum_{k=0}^{n} \binom{n}{k} 2^{nk}$ by $2^{n(n-j)}$. Due the symmetry for binomial coefficients in row n, $\binom{n}{k} = \binom{n}{n-k}$, this yields

$$\left\lfloor \frac{(2^n + 1)^n}{2^{n(n-j)}} \right\rfloor = \left\lfloor \sum_{k=0}^{j} \binom{n}{k} 2^{nk-(n(n-j))} \right\rfloor = \sum_{k=n-j}^{n} \binom{n}{k} 2^{n(n-k)} = \sum_{k=0}^{j} \binom{n}{k} 2^{nk}.$$

Next, we reduce the result of the floored division modulo $(2^n - 1)$. Viewing this sum as the polynomial $\left\lfloor \frac{(x+1)^n}{x^{n(n-j)}} \right\rfloor = \sum_{k=0}^{j} \binom{n}{k} x^k$, where x has been replaced by 2^n, we see that reducing mod $(x - 1) = (2^n - 1)$ is the same as replacing all instances of 2^n with 1 (by Ruffini's rule). Thus

$$\sum_{k=0}^{j} \binom{n}{k} 2^{nk} \bmod (2^n - 1) = \sum_{k=0}^{j} \binom{n}{k} (1)^k = \sum_{k=0}^{j} \binom{n}{k}.$$

This proves formula (i). Next, we will show that formula (ii) yields the same result. Consider

$$\left((2^n + 1)^n \bmod 2^{nj+1} \right) = \sum_{k=0}^{j} \binom{n}{k} 2^{nk}.$$

After reducing this sum mod $(2^n - 1)$ (which replaces all instances of 2^n with 1), we once again obtain $\sum_{k=0}^{j} \binom{n}{k}$. $\qquad\square$

Corollary 3.1. *Let $n, a, b \in \mathbb{Z}_{>-1}$ such that $n > 0$ and $a < b \leq n$. Then*

$$\sum_{k=a}^{b} \binom{n}{k} = \left(\left((2^n + 1)^n \bmod 2^{nb+1} \right) - \left((2^n + 1)^n \bmod 2^{na} \right) \right) \bmod (2^n - 1).$$

Proof. The proof follows trivially from Theorem 3.1, since

$$\left(\left((2^n + 1)^n \bmod 2^{nb+1} \right) - \left((2^n + 1)^n \bmod 2^{na} \right) \right) \bmod (2^n - 1)$$

$$= \sum_{k=0}^{b} \binom{n}{k} - \sum_{k=0}^{a-1} \binom{n}{k}$$

$$= \sum_{k=a}^{b} \binom{n}{k}.$$

$\qquad\square$

We now provide an alternative formula for the partial sums of binomial coefficients, using results from Boardman [11].

Theorem 3.2. *Let $n, j \in \mathbb{Z}_{>-1}$ such that $n > 0$ and $j \leq n$. Then*

$$\sum_{k=0}^{j} \binom{n}{k} = 1 + \left(\left\lfloor \frac{(2^n + 1)^n - 1}{2^{nj}(2^n - 1)} \right\rfloor \bmod 2^n \right).$$

Proof. From Boardman (2004) [11], we have the following polynomial identity:

$$\frac{(x+1)^n - 1}{x - 1} = a_1 x + a_2 x^2 + \cdots + a_n x^n = \binom{n}{1} x + \left(\binom{n}{1} + \binom{n}{2} \right) x^2 + \cdots + \left(\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \right) x^n.$$

By substituting $x = 2^n$, we obtain

$$\frac{(2^n + 1)^n - 1}{2^n - 1} = \binom{n}{1} (2^n)^1 + \left(\binom{n}{1} + \binom{n}{2} \right) (2^n)^2 + \cdots + \left(\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \right) (2^n)^n.$$

This is a valid Kronecker substitution (See § 2.2), since the largest coefficient is $a_n = \sum_{k=1}^{n} \binom{n}{k} = (2^n - 1)$ and $x = 2^n > a_n > a_{n-1} > \cdots > a_2 > a_1$.

Now, to recover $\sum_{k=1}^{j} \binom{n}{k}$, we must isolate the j-th coefficient in the sum. To achieve this, we can apply the coefficient recovery formula from Theorem 2.1. Doing so, yields

$$\left\lfloor \frac{(2^n + 1)^n - 1}{2^{nj}(2^n - 1)} \right\rfloor \bmod 2^n = \binom{n}{1} + \cdots + \binom{n}{j}.$$

Finally, we add $\binom{n}{0} = 1$ to get the desired sum, which is

$$1 + \left(\left\lfloor \frac{(2^n + 1)^n - 1}{2^{nj}(2^n - 1)} \right\rfloor \bmod 2^n \right) = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{j} = \sum_{k=0}^{j} \binom{n}{j}.$$

$\qquad\square$

4   Univariate Multinomial Coefficients

Applying Theorem 2.1, we derive a generalized formula for calculating coefficients within the multinomial expansion of arbitrary degree univariate unit polynomials. These are polynomials of the form

$$\left(\frac{x^r - 1}{x - 1}\right)^n = (x^{r-1} + \cdots + x + 1)^n.$$

The conventional approach to determine these coefficients utilizes conditional summations of multivariate multinomial coefficients, which represent the number of ways specific choices can be made to yield the term x^k [18]. The standard formula for multivariate multinomial coefficients is

$$\binom{n}{k_0, k_1, \cdots, k_{r-1}} = \frac{n!}{k_0! k_1! \cdots k_{r-1}!}.$$

In the context of our univariate polynomial, for each power of x in the expansion, the coefficient will come from all the combinations of powers that sum up to that specific power. Specifically, the coefficient of x^k in the expansion of our polynomial is [17]

$$\binom{n}{k}_{r-1} = [x^k](x^{r-1} + \cdots + x + 1)^n = \sum \binom{n}{k_0, k_1, \ldots, k_{r-1}},$$

where the summation criteria are

$$n = k_0 + k_1 + \cdots + k_{r-1},$$
$$k = 0k_0 + 1k_1 + \cdots + (r-1)k_{r-1}.$$

Theorem 4.1. *Let $n, k, r \in \mathbb{Z}$ such that $n > 0$ and $0 \leq k \leq n(r-1)$. Then*

$$\binom{n}{k}_{r-1} = \left\lfloor \left(\frac{r^{rn} - 1}{r^{n+k} - r^k}\right)^n \right\rfloor \mod r^n.$$

Proof. Consider the polynomial function

$$f_r(x)^n := \left(\frac{x^r - 1}{x - 1}\right)^n = (x^{r-1} + \cdots + x + 1)^n \in \mathbb{Z}[x].$$

In this case, it is clear that

$$f_r(1)^n = r^n.$$

Therefore, we have

$$f_r(f_r(1)^n)^n = (r^{n(r-1)} + \cdots + r^n + 1)^n.$$

Observe that the inner sum is equivalent to the summation of the powers of r^n from 0 to $(r-1)$. We note that $\sum_{k=0}^{n-1} n^k = \frac{n^n - 1}{n - 1}$. By substitution, we obtain

$$f_r(f_r(1)^n)^n = \left(\sum_{k=0}^{r-1} r^{nk}\right)^n = \left(\frac{r^{rn} - 1}{r^n - 1}\right)^n.$$

In Theorem 2.1, we showed that

$$[x^k]f(x)^n = \left\lfloor \frac{f(f(1)^n)^n}{f(1)^{nk}} \right\rfloor \mod f(1)^n.$$

In this context, we have

$$\binom{n}{k}_{r-1} = [x^k]f_r(x)^n = \left\lfloor \frac{f_r(f_r(1)^n)^n}{f_r(1)^{nk}} \right\rfloor \mod f_r(1)^n.$$

Replacing the values of $f_r(1)^n$ and $f_r(f_r(1)^n)^n$ and simplifying, we arrive at our original formula

$$\binom{n}{k}_{r-1} = [x^k]\left(\frac{x^r - 1}{x - 1}\right)^n = \left\lfloor \left(\frac{r^{rn} - 1}{r^n - 1}\right)^n r^{-nk} \right\rfloor \mod r^n = \left\lfloor \left(\frac{r^{rn} - 1}{r^{n+k} - r^k}\right)^n \right\rfloor \mod r^n,$$

completing the proof. □

4.1 Partial Sums of Univariate Multinomial Coefficients

As a corollary, we will now prove a formula for the partial sums of univariate multinomial coefficients, taking a similar approach as in § 3.

Corollary 4.1. *Let $n, j, r \in \mathbb{Z}^+$ such that $n > 0$ and $0 \leq j \leq n(r-1)$. Then*

$$\sum_{k=0}^{j} \binom{n}{k}_{r-1} = \left(\left(\frac{r^{rn} - 1}{r^n - 1} \right)^n \bmod r^{n(j+1)} \right) \bmod (r^n - 1).$$

Proof. First, we note that $\left(\frac{r^{nr}-1}{r^n} \right)^n = \sum_{k=0}^{n} \binom{n}{k}_{r-1} r^{nk}$. Reducing the sum mod $r^{n(j+1)}$, we get

$$\sum_{k=0}^{j} \binom{n}{k}_{r-1} r^{nk}.$$

Finally, reducing this sum mod $(r^n - 1)$ is the same as replacing all instances of r^n with 1, leading to

$$\sum_{k=0}^{j} \binom{n}{k}_{r-1} r^{nk} \bmod (r^n - 1) = \sum_{k=0}^{j} \binom{n}{k}_{r-1} (1)^k = \sum_{k=0}^{j} \binom{n}{k}_{r-1}.$$

$\square$

5 Solution to an Open Problem

The coefficients of the term x^n in the polynomial expansion of $(x^2 + x + 1)^n$, denoted as $\binom{n}{n}_2$, are known as the **central trinomial coefficients** (sequence A002426 in the OEIS). Applying our univariate multinomial coefficient formula from Theorem 4.1, we see that

$$\binom{n}{n}_2 = \left\lfloor \left(\frac{3^{3n} - 1}{3^{2n} - 3^n} \right)^n \right\rfloor \bmod 3^n = \left\lfloor \left(\frac{27^n - 1}{9^n - 3^n} \right)^n \right\rfloor \bmod 3^n.$$

Starting from $n = 1$, the sequence begins as

$$1, 3, 7, 19, 51, 141, 393, 1107, 3139, 8953, 25653, 73789, 212941, 616227, 1787607, 5196627, \ldots.$$

A **hypergeometric closed form** is a linear combination, with respect to a field K, of expressions $f(n)$ such that $\frac{f(n+1)}{f(n)}$ is a rational function on K [12, 22].

As is the case with the partial sums of binomial coefficients (See § 3), it was proved by Petkovšek et al. that there is no hypergeometric closed form for the central trinomial coefficients [12]. Based on this result, Graham et al. posed a related research problem [18]:

Problem 5.1. *Prove that there is no "simple closed form" for the coefficient of x^n in $(x^2 + x + 1)^n$, as a function of n, in some large class of simple closed forms.*

Here, a "simple closed form" is defined as an expression using only addition, subtraction, multiplication, division, and exponentiation [18]. This is essentially the definition of a Kalmar function. We will demonstrate that no such class exists, thereby providing a negative solution to the problem posed by Graham et al.

5.1 Proofs

Given an integer c, let $||c||$ denote one plus the length of the bit-string encoding c (we add one unit in order to make the bounds of the following proofs clearer).

Let CT be the function which maps any univariate expression into its computation time. It is well-known that, if m, u and v are integers such that $v \neq 0$ and $m = \max(||u||, ||v||)$, then $\mathrm{CT}(u+v)$, $\mathrm{CT}(uv)$ and $\mathrm{CT}(u/v)$ are upper-bounded by m, m^2 and $m^2 \log(m)$, respectively.

Given a rational number q and two coprime integers $b > 0$ and a such that $q = a/b$, let $\mathcal{N}(q)$ and $\mathcal{D}(q)$ denote the numbers a and b, respectively.

The following two results are due to Mihai Prunescu and Lorenzo Sauras-Altuzarra (pers. comm.):

Lemma 5.1. *If $s(n)$ is a hypergeometric term on $\mathbb{Q}$ and $s(k) \neq 0$ for every integer $k \geq 0$, then $\mathrm{CT}(s(n))$ is upper-bounded by some expression of the form $2^{2^{\cdot^{\cdot^{\cdot^{2^{||n||}}}}}}$.*

Proof. Let $f(n) = \frac{s(n+1)}{s(n)}$. Since $s(n)$ is hypergeometric, $f(n) \in \mathbb{Q}(n)$. Thus, there exists a positive integer r such that $\mathcal{N}(f(n))$ and $\mathcal{D}(f(n))$ are upper-bounded by n^r.

For every non-negative integer k such that $||k|| \leq ||n||$, there exist functions $g(||n||)$ and $h(||n||)$ such that $||\mathcal{N}(f(k))||$ and $||\mathcal{D}(f(k))||$ are upper-bounded by $g(||n||)$, and $\mathrm{CT}(\mathcal{N}(f(k)))$ and $\mathrm{CT}(\mathcal{D}(f(k)))$ are upper-bounded by $h(||n||)$.

For large n, we have

$$\mathrm{CT}\left(\frac{s(n)}{s(0)}\right) = \mathrm{CT}\left(\prod_{k=0}^{n-1} f(k)\right) \leq \mathrm{CT}\left(\frac{\prod_{k=0}^{n-1} \mathcal{N}(f(k))}{\prod_{k=0}^{n-1} \mathcal{D}(f(k))}\right) \leq$$

$$\sum_{k=0}^{n-1} \mathrm{CT}(\mathcal{N}(f(k))) + \sum_{j=2}^{n} \mathrm{CT}\left(\prod_{k=0}^{j-1} \mathcal{N}(f(k))\right) + \sum_{k=0}^{n-1} \mathrm{CT}(\mathcal{D}(f(k))) + \sum_{j=2}^{n} \mathrm{CT}\left(\prod_{k=0}^{j-1} \mathcal{D}(f(k))\right) + \mathrm{CT}\left(\frac{\prod_{k=0}^{n-1} \mathcal{N}(f(k))}{\prod_{k=0}^{n-1} \mathcal{D}(f(k))}\right) \leq$$

$$nh(||n||)+$$
$$\max(||\mathcal{N}(f(0))||, ||\mathcal{N}(f(1))||)^2+$$
$$\max(||\mathcal{N}(f(0))\mathcal{N}(f(1))||, ||\mathcal{N}(f(2))||)^2 + \cdots +$$
$$\max(||\mathcal{N}(f(0))\mathcal{N}(f(1)) \cdots \mathcal{N}(f(n-2))||, ||\mathcal{N}(f(n-1))||)^2+$$
$$nh(||n||)+$$
$$\max(||\mathcal{D}(f(0))||, ||\mathcal{D}(f(1))||)^2+$$
$$\max(||\mathcal{D}(f(0))\mathcal{D}(f(1))||, ||\mathcal{D}(f(2))||)^2 + \cdots +$$
$$\max(||\mathcal{D}(f(0))\mathcal{D}(f(1)) \cdots \mathcal{D}(f(n-2))||, ||\mathcal{D}(f(n-1))||)^2+$$
$$\max(||\mathcal{N}(f(0)) \cdots \mathcal{N}(f(n-1))||, ||\mathcal{D}(f(0)) \cdots \mathcal{D}(f(n-1))||)^2 \cdot$$
$$\log(\max(||\mathcal{N}(f(0)) \cdots \mathcal{N}(f(n-1))||, ||\mathcal{D}(f(0)) \cdots \mathcal{D}(f(n-1))||)) \leq$$

$$2nh(||n||) + 2(1g(||n||))^2 + 2(2g(||n||))^2 + \cdots + 2(ng(||n||))^2 + (ng(||n||))^2 \log(ng(||n||)) =$$
$$2nh(||n||) + 2(1^2 + 2^2 + \cdots + n^2)g(||n||)^2 + n^2 g(||n||)^2 \log(ng(||n||)) =$$
$$2nh(||n||) + n(n+1)(2n+1)g(||n||)^2/3 + n^2 g(||n||)^2 \log(ng(||n||)).$$

The last expression is upper-bounded by some arithmetic term, thus $\mathrm{CT}(s(n))$ is upper-bounded by $2^{2^{\cdot^{\cdot^{\cdot^{2^{||n||}}}}}}$. $\square$

Theorem 5.1. *If r is a non-negative integer and $s_0(n), \ldots, s_r(n)$ are hypergeometric terms on $\mathbb{Q}$ such that $s_i(j) \neq 0$ for every two non-negative integers $i \leq r$ and j, then $\mathrm{CT}(s_0(n) + \ldots + s_r(n))$ is upper-bounded by some expression of the form $2^{2^{\cdot^{\cdot^{\cdot^{2^{||n||}}}}}}$.*

Proof. Lemma 5.1 implies the existence of an expression $M(n)$, of the form $2^{2^{\cdot^{\cdot^{\cdot^{2^{||n||}}}}}}$, such that, for every $i \in \{0, \ldots, r\}$, $s_i(n)$ and $\mathrm{CT}(s_i(n))$ are upper-bounded by $M(n)$.

Therefore, for large enough values of n, we have that

$$\mathrm{CT}\left(\sum_{k=0}^{r} s_k(n)\right) \leq \sum_{j=0}^{r} \mathrm{CT}\left(\sum_{k=0}^{j} s_k(n)\right) \leq \sum_{k=0}^{r} \mathrm{CT}(s_k(n))+$$

$$\max(||s_0(n)||, ||s_1(n)||)+$$
$$\max(||s_0(n) + s_1(n)||, ||s_2(n)||) + \cdots +$$
$$\max(||s_0(n) + s_1(n) + s_2(n) + \cdots + s_{r-1}(n)||, ||s_r(n)||)$$
$$\leq rM(n) + M(n) + 2M(n) + \cdots + rM(n)$$
$$= rM(n) + r(r+1)M(n)/2.$$

And the expression is clearly upper-bounded by some expression of the form $2^{2^{\cdot^{\cdot^{\cdot^{2^{||n||}}}}}}$. $\square$

This theorem allows us to establish the following corollaries:

Corollary 5.1. *Let C be a class of integer-valued functions that is Kalmar and contains functions $f(n)$ such that the ratio of consecutive terms $\frac{f(n+1)}{f(n)}$ is irrational on C. Then, C contains the central trinomial coefficients.*

Proof. Let $s(n)$ be the sequence of central trinomial coefficients, which are the coefficients of x^n in the expansion of $(x^2 + x + 1)^n$. From Theorem 4.1, these coefficients can be expressed using the Kalmar formula

$$s(n) = \left\lfloor \left(\frac{27^n \dot{-} 1}{9^n \dot{-} 3^n} \right)^n \right\rfloor \bmod 3^n.$$

All functions in C are integer-valued, so C does not contain any functions that directly return irrational or transcendental numbers. However, since C is Kalmar, any real number can be approximated to arbitrary precision by a sequence of the form $\lim_{n \to \infty} \frac{f(n+1)}{f(n)}$, where $f(n) \in C$. This is true because irrational and transcendental numbers can be approximated by rational numbers, and rational approximations can be derived from generalized continued fractions, which are defined by recurrence relations involving only integer arithmetic operations. These operations fall within the scope of Kalmar functions, thereby allowing the sequence in C to approximate any real number to arbitrary precision.

Since C contains the $\lfloor a/b \rfloor$ operation, which can be interpreted as rational division followed by rounding down to the nearest integer, we see that the quotient in the limit can be calculated to arbitrary precision and converted an integer. Since C is Kalmar, this limit can be approximated as some function of n that is bounded by $2^{2^{\cdots^{2^n}}}$. Therefore, $s(n)$ is contained within C. $\square$

Corollary 5.2. *Problem 5.1 has no solutions.*

Proof. From Corollary 5.1, we see that any solution to the problem posed by Graham et al. (Problem 5.1), which is a class of Kalmar functions C (by Theorem 4.1 and Theorem 5.1), must either contain the hypergeometric restriction or weakened variant of it. Therefore, we conclude that Problem 5.1 has no solutions. $\square$

6 Acknowledgements

References

[1] A. Greuet, S. Montoya, and C. Vermeersch. Modular Polynomial Multiplication Using RSA/ECC coprocessor. Cryptology ePrint Archive, Paper 2022/879, 2022. URL https://eprint.iacr.org/2022/879.

[2] A. Grzegorczyk. Some Classes of Recursive Functions. *Rozprawy Matematyczne*, 4, 1953. URL http://matwbn.icm.edu.pl/ksiazki/rm/rm04/rm0401.pdf.

[3] D. Harvey. Faster Polynomial Multiplication via Multipoint Kronecker Substitution. *Journal of Symbolic Computation*, 44, 2009. doi: 10.1016/j.jsc.2009.05.004.

[4] D. Harvey and J. van der Hoeven. Faster Polynomial Multiplication Over Finite Fields Using Cyclotomic Coefficient Rings. *Journal of Complexity*, 54, 2019. ISSN 0885-064X. URL https://www.sciencedirect.com/science/article/pii/S0885064X19300378.

[5] G. T. Herman. A New Hierarchy of Elementary Functions. *Proceedings of the American Mathematical Society*, 20(2):557–562, 1969. ISSN 0002-9939.

[6] OEIS Foundation Inc. Powers of 2 - Entry A000079 in The On-Line Encyclopedia of Integer Sequences, 2024. URL https://oeis.org/A000079.

[7] J. D. Cook. Polynomial Determined by Two Inputs, 2012. URL https://johndcook.com/blog/2012/03/27/polynomial-trick. Blog Post.

[8] J. Robinson. Existential Definability in Arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. ISSN 0002-9947.

[9] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013. ISBN 978-1107039032.

[10] J. W. Bos, J. Renes, and C. van Vredendaal. Post-Quantum Cryptography with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen and Nussbaumer. Cryptology ePrint Archive, Paper 2020/1303, 2020. URL https://eprint.iacr.org/2020/1303.

[11] M. Boardman. The Egg-Drop Numbers. *Mathematics Magazine*, 77(5):368–372, 2004. URL https://doi.org/10.1080/0025570X.2004.11953281.

[12] M. Petkovšek, H. S. Wilf, and D. Zeilberger. *A=B*. A K Peters/CRC Press, 1996. ISBN 978-1568810638.

[13] M. Prunescu and L. Sauras-Altuzarra. An Arithmetic Term for the Factorial Function. *Examples and Counterexamples*, 5, 2024. ISSN 2666-657X. URL https://sciencedirect.com/science/article/pii/S2666657X24000028.

[14] M. R. Albrecht, C. Hanser, A. Hoeller, T. Pöppelmann, F. Virdia, and A. Wallner. Implementing RLWE-based Schemes Using an RSA Co-Processor. Cryptology ePrint Archive, Paper 2018/425, 2018. URL https://eprint.iacr.org/2018/425.

[15] MathOverflow Users. Application of Polynomials with Non-Negative Coefficients, 2012. URL https://mathoverflow.net/questions/91827. MathOverflow Discussion.

[16] M. Prunescu and L. Sauras-Altuzarra. On the Representation of C-Recursive Integer Sequences by Arithmetic Terms, 2024. URL https://arxiv.org/abs/2405.04083.

[17] R. A. Brualdi. *Introductory Combinatorics*. Pearson, 5th edition, 2017. ISBN 978-0134689616.

[18] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation For Computer Science*. Addison-Wesley Professional, 2nd edition, 1994. ISBN 978-0201558029.

[19] Reddit Users. Determine a Polynomial from Just Two Inputs, 2023. URL https://www.reddit.com/r/math/comments/yx0i7r/determine_a_polynomial_from_just_two_inputs. Reddit Discussion.

[20] S. Mazzanti. Plain Bases for Classes of Primitive Recursive Functions. *Mathematical Logic Quarterly*, 48(1):93–104, 2002. ISSN 0942-5616.

[21] S. S. Marchenkov. Superpositions of Elementary Arithmetic Functions. *Journal of Applied and Industrial Mathematics*, 1(3): 351–360, 2007. ISSN 1990-4789.

[22] L. Sauras-Altuzarra. Hypergeometric Closed Forms, 2018. URL https://www.mat.univie.ac.at/~kratt/theses/sauras.pdf.

[23] Wikipedia Contributors. Binomial Coefficient, 2024. URL https://en.wikipedia.org/wiki/Binomial_coefficient. Wikipedia Article.

[24] Y. Matiyasevich. A New Proof of the Theorem on Exponential Diophantine Representation of Enumerable Sets. *Journal of Soviet Mathematics*, 14(5):1475–1486, 1980. ISSN 0090-4104.