J Autom Reasoning (2019) 62:171–192
https://doi.org/10.1007/s10817-017-9438-0

Proof Pearl: Bounding Least Common Multiples with Triangles

Hing-Lun Chan[2] · **Michael Norrish**[1,2]

Received: 9 February 2017 / Accepted: 23 September 2017 / Published online: 14 October 2017

Abstract We present a proof of the fact that $2^n \leq \mathsf{LCM}\{1, 2, 3, \ldots, (n + 1)\} \leq 4^{(n + 1)}$ for $n \geq 0$. This result has a standard proof via an integral, but our proof is purely number-theoretic, requiring little more than inductions based on lists. The almost-pictorial proof is based on manipulations of a variant of Leibniz's harmonic triangle, itself a relative of Pascal's better-known Triangle.

Keywords Least common multiple · Pascal's triangle · Leibniz's triangle · Formalisation · Automated theorem proving · HOL4 · Binomial coefficients

1 Introduction

The least common multiple (LCM) of consecutive natural numbers is bounded:

$$2^n \leq \mathsf{LCM}\{1, 2, 3, \ldots, n\} \leq 4^n \quad \text{with } n \geq 7 \text{ for the lower bound}$$

The lower bound is a minor (though important) part of the complexity proof of the Agrawal–Kayal–Saxena-algorithm (AKS) for "PRIMES is in P" (see below for more motivational detail). A short proof is given by Nair [18], based on a sum expressed as an integral. That paper ends with these words:

> It also seems worthwhile to point out that there are different ways to prove the identity implied [...], for example, [...] by using the difference operator.

✉ Hing-Lun Chan
joseph.chan@anu.edu.au

Michael Norrish
Michael.Norrish@data61.csiro.au

[1] Data61, CSIRO, Canberra, Australia

[2] Australian National University, Canberra, Australia

Nair's remark indicates the possibility of an elementary proof of the above number-theoretic results. Nair's integral turns out to be an expression of the beta-function, and there is a little-known relationship between the beta-function and Leibniz's harmonic triangle (see Ayoub [4]). The harmonic triangle can be described as the difference table of the harmonic sequence: $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$ (e.g., as presented in Bicknell-Johnson [5]).

Exploring this connection, we work out interesting proofs of these results that are both clear and elegant. Although the idea has been sketched in various sources (e.g., [17]), we put the necessary pieces together in a coherent argument, and prove them formally in HOL4.

Extension This paper is a complete rework of our earlier conference paper [7], which only proves the weaker result:

$$2^n \leq \mathsf{LCM}\{1, 2, 3, \ldots, (n + 1)\} \quad \text{for } n \geq 0.$$

Though this is sufficient for our AKS work, we show how Leibniz's harmonic triangle can be applied to prove the stronger result (Sect. 6.1), using a technique implicit in Nair's paper. Following Nair, we also obtain the upper bound (Sect. 7). To wrap up, we relate the LCM bounds to current formalization work (Sect. 8).

Overview We find that the rows of denominators in Leibniz's harmonic triangle provide a trick to enable an estimation of the lower bound of the LCM of consecutive numbers. The route from this row property to the desired bound is subtle: we exploit an LCM exchange property for triplets of neighboring elements in the denominator triangle. We shall show how this property gives a wonderful proof of the weak LCM lower bound for consecutive numbers in HOL4:

Theorem 1 *A lower bound for the LCM of consecutive numbers.*

$$\vdash\ 2^n \leq \mathsf{list\_lcm}\ [1\ ..\ n + 1]$$

where list_lcm *is the obvious extension of the binary* lcm *operator to a list of numeric arguments.*

Moreover, we discover that the principle behind the proof of Theorem 1 can squeeze this out:

Theorem 2 (Nair) *A better lower bound for the LCM of consecutive numbers.*

$$\vdash\ 7 \leq n \Rightarrow 2^n \leq \mathsf{list\_lcm}\ [1\ ..\ n]$$

Furthermore, using an idea of Nair, we derive:

Theorem 3 (also Nair) *An upper bound for the LCM of consecutive numbers.*

$$\vdash\ \mathsf{list\_lcm}\ [1\ ..\ n] \leq 4^n$$

This upper bound is discussed further in Sect. 8.

Motivation This work was initiated as part of our mechanization work of the AKS algorithm [1], the first unconditionally deterministic polynomial-time algorithm for primality testing. As part of its initial action, the AKS algorithm searches for a parameter k satisfying a condition dependent on the input number. The major part of the AKS algorithm then involves a for-loop whose count depends on the size of k.

In our first paper [6] on the correctness (but not complexity) of the AKS algorithm, we proved the existence of such a parameter k on general grounds, but did not provide a bound.

In order to show the complexity result for the AKS algorithm, we must provide a tight bound on k. As indicated in the AKS paper [1, Lemma 3.1], the necessary bound on k can be derived from a lower bound on the LCM of consecutive numbers.[1]

Historical Notes Pascal's arithmetic triangle (c1654) is well-known,[2] but Leibniz's harmonic triangle (1672) has comparatively been neglected. As reported by Massa Esteve and Delshams [10], in 1659 Pietro Mengoli investigated certain sums of a special form, using a combinatorial triangle identical to the harmonic triangle. Those special sums are the basis of Euler's beta-function (1730) defined by an integral.

In another vein, Hardy and Wright's *Theory of Numbers* [14] related the LCM lower bound of consecutive numbers to the Prime Number Theorem (more information in Sect. 8), which work was followed up by Nair [18], giving the bounds in Theorems 2 and 3 through a clever application of the beta-function.

Our approach to prove Theorem 1 is inspired by Farhi [11], in which a certain binomial coefficient identity, equivalent to our Theorem 14, was established using Kummer's theorem. A direct computation to relate both results of Nair and Farhi was given by Hong [16].

Paper Structure The rest of this paper is devoted to explaining the mechanised proofs of Theorems 1, 2 and 3. We give some background to Pascal's and Leibniz's triangles in Sect. 2. Section 3 discusses two forms of the Leibniz's triangle: the harmonic form and the denominator form, and Sect. 4 proves the important LCM exchange property for our Leibniz triplets. Section 5 shows how paths in the denominator triangle can make use of the LCM exchange property, eventually proving that both the consecutive numbers and a row of the denominator triangle share the same LCM. In Sect. 6, we apply this LCM relationship to give a proof of Theorem 1. Section 6.1 goes further with the LCM exchange property to give a formal proof of Theorem 2. Adapting an idea in Nair's paper to our triangles, we formalise Theorem 3 in Sect. 7. We discuss some formalization work related to this topic in Sect. 8, and conclude in Sect. 9.

HOL4 Notation All statements starting with a turnstile ($\vdash$) are HOL4 theorems, automatically pretty-printed to LaTeX from the relevant theory in the HOL4 development. Generally, our notation allows an appealing combination of quantifiers ($\forall$, $\exists$), logical connectives ($\wedge$ for "and", $\neg$ for "not", $\Rightarrow$ for "implies", and $\iff$ for "if and only if"). Sets are enclosed in curly-brackets {}, with set elements separated by comma (,). Lists are enclosed in square-brackets [ ], with list members separated by semicolon (;), using infix operators :: for "cons", $\frown$ for append, and . . for inclusive range. Common list operators are: LENGTH, SUM, $\mathsf{REVERSE}$, MEM for list member, and others to be introduced as required. Given a binary relation $\mathcal{R}$, its reflexive and transitive closure is marked by an asterisk ($*$), i.e., $\mathcal{R}^*$.

Throughout this paper, arithmetic over the natural numbers will be used: when $b \leq a$, $b - a = 0$ since it is truncated subtraction. The integer quotient of a divided by b is denoted by $\lfloor a \div b \rfloor$ or $\lfloor a/b \rfloor$. The integer functions used are: lcm for least common multiple, gcd for greatest common divisor, and $n!$ for factorial of n.

HOL4 Sources Our proof scripts, consisting of Binomial Theory, Triangle Theory and supporting libraries, can be found at https://bitbucket.org/jhlchan/hol/src/, in the sub-folder

[1] The AKS paper [1] cites Nair's tighter LCM lower bound (Theorem 2), but as our forthcoming AKS formalization paper shows, the weaker LCM lower bound of Theorem 1 suffices.

[2] The pattern of binomial expansion for successive powers is known from antiquity, as recorded in mathematical treatises from China, Japan, India, as well as Arabic countries. For a full history of the arithmetic triangle, see Edwards [9].

Table 1 The consecutive LCM function $L(n)$, comparing with various bounds

n	2^{n-1}	2^n	$L(n)$	4^n
0	1	1	1	1
1	1	2	1	4
2	2	4	2	16
3	4	8	6	64
4	8	16	12	256
5	16	32	60	1024
6	32	64	60	4096
7	64	128	420	16384
8	128	256	840	65536
9	256	512	2520	262144
10	512	1024	2520	1048576

algebra/lib. These sources, with the tag `jar2017-lcm-revised02`, can be built with HOL4 at `git` commit `5765cb0a` (released June 2017).

2 Background

2.1 The Consecutive LCM Function

Let $L(n) = \mathsf{LCM}\{1, 2, \ldots, n\}$, the least common multiple of the consecutive numbers from 1 to n. We define $L(0) = 1$ to obtain the recurrence $L(n + 1) = \mathsf{lcm}(n + 1, L(n))$. This enables easy computations of successive values of $L(n)$. Theorem 2 says $2^n \leq L(n)$ for $n \geq 7$, while Theorems 1 and 3 together assert that $2^{n-1} \leq L(n) \leq 4^n$ for all n.[3] The initial values of $L(n)$ are shown in Table 1 (see also Fig. 9).

Taking $L(n)$ as a function of n, we can see how it grows. In fact, the recurrence formula shows that $L(n)$ divides $L(n + 1)$. With $L(0) = 1$, $L(n)$ is always positive. Therefore $L(n)$ is monotonic, with each term dividing the next.

To obtain its bounds, it is useful to treat $L(n)$ as dependent on all the consecutive numbers up to n. As noted, we make use of the list $[1 \;..\; n]$ to represent these consecutive numbers.[4]

Definition 4 We define $L(n) = \mathsf{list\_lcm}\ [1 \;..\; n]$ in HOL4, with:

$$\begin{aligned} \mathsf{list\_lcm}\ [\,] &= 1 \\ \mathsf{list\_lcm}\ (h :: t) &= \mathsf{lcm}(h, \mathsf{list\_lcm}\ t) \end{aligned}$$

First we verify this (refer to *HOL4 Notation*):

[3] Note that for integer arithmetic, $2^{0-1} = 2^0 = 1$.

[4] Another representation is based on sets. The set elements are indexed by natural numbers, so that elements can be swapped. This approach was shown to us (personal communication) by Laurent Théry. Our source script file Triangle includes a proof of Theorem 1 based on this alternative approach.

Lemma 5 *The* list_lcm *is a common multiple, and the least common multiple, of all the members of a list.*

$$\vdash \ \mathsf{MEM}\ x\ \ell \ \Rightarrow\ x \mid \mathsf{list\_lcm}\ \ell$$
$$\vdash \ (\forall x.\ \mathsf{MEM}\ x\ \ell \ \Rightarrow\ x \mid m) \ \Rightarrow\ \mathsf{list\_lcm}\ \ell \mid m$$

Next we prove:

Lemma 6 *Some simple properties of* list_lcm.

- *The* list_lcm *of two parts is the* LCM *of the* list_lcm *of each part.*

$$\vdash \ \mathsf{list\_lcm}\ (l_1 \frown l_2) \ = \ \mathsf{lcm}(\mathsf{list\_lcm}\ l_1, \mathsf{list\_lcm}\ l_2)$$

- *The* list_lcm *of a reverse list is the same as that of the original list.*

$$\vdash \ \mathsf{list\_lcm}\ (\mathsf{REVERSE}\ \ell) \ = \ \mathsf{list\_lcm}\ \ell$$

We shall generalize the problem of finding “what are the bounds for $L(n)$?” to this one: given a list ℓ of positive numbers, what are the lower and upper bounds for list_lcm ℓ ? Such a list is called a *positive* list, denote by $\mathsf{POSITIVE}\ \ell \iff \forall x.\ \mathsf{MEM}\ x\ \ell \Rightarrow 0 < x$.

2.2 LCM Lower Bound for a List

The following observation is simple:

Theorem 7 *The least common multiple of a non-empty positive list cannot be less than their integer average.*

$$\vdash \ \ell \neq [\,] \ \wedge\ \mathsf{POSITIVE}\ \ell \ \Rightarrow\ \lfloor \mathsf{SUM}\ \ell \div \mathsf{LENGTH}\ \ell \rfloor \ \leq\ \mathsf{list\_lcm}\ \ell$$

Proof Let $m = \mathsf{list\_lcm}\ \ell$, and $z = \mathsf{LENGTH}\ \ell$. Each member $x_i \mid m$, or $x_i \leq m$ since $m \neq 0$. Then:

$$\mathsf{SUM}\ \ell = \sum_{i=1}^{z} x_i \ \leq\ \sum_{i=1}^{z} m = z \times m.$$

With $\ell \neq [\,]$, its length $z \neq 0$. A simple integer division gives the desired result. □

A naïve application of this result to the list $[1\ ..\ n+1]$ gives a disappointing LCM lower bound. For an ingenious use to obtain Theorem 1, we turn to Leibniz’s Triangle, a close relative of Pascal’s Triangle.

2.3 Pascal’s Triangle

Pascal’s well-known triangle (refer to Fig. 1) can be described as follows:

- Each boundary entry: always 1.
- Each inside entry: sum of two immediate parents.

This gives the classic top-down row-by-row construction of Pascal’s triangle (refer to Fig. 1).

Entries of Pascal’s triangle (the k-th element on n-th row) are binomial coefficients $\binom{n}{k}$, which is defined to be zero when $k > n$. The binomial expansion of $(1 + 1)^n$ gives the n-th row sum: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Since Leibniz’s triangle (see Sect. 2.4 below) will be defined using Pascal’s triangle, we include the binomials as a foundation in our HOL4 implementation, proving the above result:

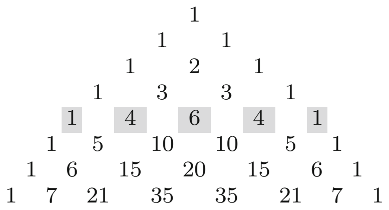

Fig. 1 Pascal's Arithmetic Triangle: with a horizontal row indicated

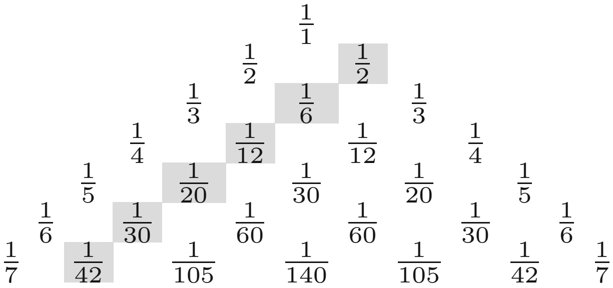

Fig. 2 Leibniz's Harmonic Triangle: with a slanting column indicated

Theorem 8 *The sum along the n-th row in Pascal's Triangle is 2^n.*

$$\vdash \ \mathsf{SUM}\ (\mathcal{P}_{\text{row}}\ \ n) \ = \ 2^n$$

We use $(\mathcal{P}_{\text{row}}\ \ n)$ to represent the n-th row of Pascal's triangle, counting n from 0.

2.4 Leibniz's Harmonic Triangle

Leibniz's harmonic triangle (refer Fig. 2) can be described similar to Pascal's triangle:

- Each boundary entry: $\dfrac{1}{(n+1)}$ for the n-th row, with n starting from 0.
- Each entry (inside or not): sum of two immediate children.

This builds the Leibniz triangle from the left boundary, in slanting columns parallel to the boundary, using subtraction after carefully identifying the children associated with the node.

Note that the boundary entries form the well-known harmonic sequence, which gives rise to its name. This Leibniz's triangle is closely related to Pascal's triangle. Indeed, let $\begin{bmatrix} n \\ k \end{bmatrix}$ be the k-th element on n-th row of the harmonic triangle, it can be shown (e.g., see Ayoub [4]) from the construction rules that:

- Explicit expression for an entry: $\begin{bmatrix} n \\ k \end{bmatrix} = \dfrac{1}{(n+1)\binom{n}{k}}$
- Weighted row sum by binomials: $\displaystyle\sum_{k=0}^{n} \binom{n}{k} \begin{bmatrix} n \\ k \end{bmatrix} = 1$

Since all entries of the harmonic triangle are unit fractions, we can pick only the denominators of the entries to form Leibniz's "Denominator Triangle." This allows us to deal with just whole numbers in HOL4.

						1						
					2		2					
				3		6		3				
			4		12		12		4			
		5		20		30		20		5		
	6		30		60		60		30		6	
7		42		105		140		105		42		7

row n \ column k:	0	1	2	3	4	5	6
$n = 0$	1						
$n = 1$	2	2					
$n = 2$	3	6	3				
$n = 3$	4	12	12	4			
$n = 4$	5	20	30	20	5		
$n = 5$	6	30	60	60	30	6	
$n = 6$	7	42	105	140	105	42	7

Fig. 3 Leibniz's Denominator Triangle: symmetrical and rectangular

3 Leibniz's Denominator Triangle

The denominators of each entry of Leibniz's Harmonic Triangle form the Denominator Triangle, denoted by $\mathcal{L}$. We define its entries *via* the binomial coefficients in HOL4:

Definition 9 The denominator form of Leibniz's triangle: entry at n-th row, k-th column.

$$\mathcal{L}\ n\ k\ =\ (n\ +\ 1)\ \times\ \binom{n}{k}$$

Note that $\mathcal{L}\ \ n\ \ k\ =\ 0$ when $k\ >\ n$, since in this case $\binom{n}{k}\ =\ 0$ by definition.

Figure 3 shows the first few rows of the Denominator Triangle, with the rectangular format on the right. The rectangular format keeps the rows on the left, but shifts the left boundary to be vertical. Evidently from Definition 9, the left boundary (shaded vertical) consists of consecutive numbers, from the denominators of the harmonic sequence:

$$\vdash\ \ \mathcal{L}\ n\ 0\ =\ n\ +\ 1$$

Denoting the n-th row (shaded horizontal) by $\mathcal{L}_{\text{row}}\ \ n$, we have:

Theorem 10 *The integer average of the n-th row of Leibniz's denominator triangle is* 2^n.

$$\vdash\ \ \lfloor \mathsf{SUM}\ (\mathcal{L}_{\text{row}}\ \ n) \div \mathsf{LENGTH}\ (\mathcal{L}_{\text{row}}\ \ n) \rfloor\ =\ 2^n$$

Proof From Definition 9, $(\mathcal{L}_{\text{row}}\ \ n)$ is just a multiple of $(\mathcal{P}_{\text{row}}\ \ n)$ by a factor of $(n\ +\ 1)$, giving:

$$\vdash\ \ \mathsf{SUM}\ (\mathcal{L}_{\text{row}}\ \ n)\ =\ (n\ +\ 1)\ \times\ \mathsf{SUM}\ (\mathcal{P}_{\text{row}}\ \ n)$$
$$\vdash\ \ \mathsf{LENGTH}\ (\mathcal{L}_{\text{row}}\ \ n)\ =\ n\ +\ 1$$

The result follows by applying the binomial sum formula of Theorem 8. □

The insight provided by Leibniz's Denominator Triangle is this: if only list_lcm $[1\ \ ..\ \ n\ +\ 1]$ were the same as list_lcm $(\mathcal{L}_{\text{row}}\ \ n)$, we would have Theorem 1 directly from Theorems 7 and 10. Is this just a dream?

4 Leibniz Triplet

In the Denominator Triangle shown on the right of Fig. 3, the shaded vertical and horizontal arms form a big L-shape. To explore whether the overall LCM of the vertical arm can possibly equal the overall LCM of the horizontal arm, we shall zoom in to investigate the building blocks. These are the smallest L-shapes in the Denominator Triangle, shown in Table 2.

Table 2 Denominator Triangle in vertical-horizontal form, with a typical triplet marked

Row n\column k	$k=0$,	$k=1$,	$k=2$,	$k=3$,	$k=4$,	$k=5$,	$k=6$,	…
$n=0$	1							
$n=1$	2	2						
$n=2$	3	6	3					
$n=3$	4	12	12	4				
$n=4$	5	20	30	20	5			
$n=5$	6	30	60	60	30	6		
$n=6$	7	42	105	140	105	42	7	

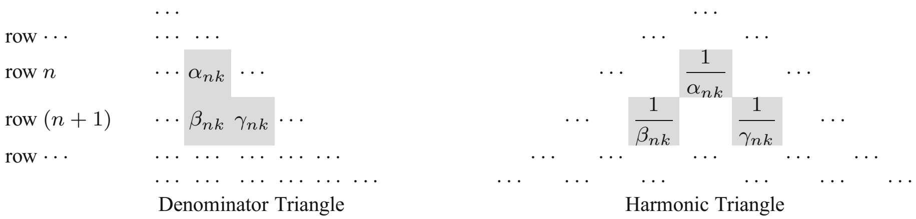

Fig. 4 The Leibniz triplet: location in Denominator Triangle and origin in Harmonic Triangle

Within this vertical-horizontal format, we identify L-shaped "Leibniz triplets" (a typical one is marked) rooted at row n and column k, with 3 entries:

- the root of the triplet: $\alpha_{nk} = \mathcal{L}\ n\ k$ and,
- its two children on the next row: $\beta_{nk} = \mathcal{L}\ (n+1)\ k$, $\gamma_{nk} = \mathcal{L}\ (n+1)\ (k+1)$

Note that the values α_{nk}, β_{nk} and γ_{nk} occur as denominators in Leibniz's original harmonic triangle, corresponding to the situation that the entry $\frac{1}{\alpha_{nk}}$ has immediate children $\frac{1}{\beta_{nk}}$ and $\frac{1}{\gamma_{nk}}$ (refer to Fig. 4). By the construction rule of the harmonic triangle, we should have:

$$\frac{1}{\alpha_{nk}} = \frac{1}{\beta_{nk}} + \frac{1}{\gamma_{nk}}, \quad \text{or} \quad \frac{1}{\gamma_{nk}} = \frac{1}{\alpha_{nk}} - \frac{1}{\beta_{nk}}$$

which, upon clearing fractions, becomes:

$$\alpha_{nk} \times \beta_{nk} = \gamma_{nk} \times (\beta_{nk} - \alpha_{nk})$$

Indeed, our definition of $(\mathcal{L}\ n\ k)$ satisfies this property:

Theorem 11 *An identity for a Leibniz triplet in the Denominator Triangle.*

$$\vdash \alpha_{nk} \times \beta_{nk} = \gamma_{nk} \times (\beta_{nk} - \alpha_{nk})$$

Proof Definition 9 leads to these relationships for the vertical and horizontal pairs of the triplet:

$$\vdash (n + 2) \times \alpha_{nk} = (n + 1 - k) \times \beta_{nk} \qquad \text{vertical pair}$$
$$\vdash (k + 1) \times \gamma_{nk} = (n + 1 - k) \times \beta_{nk} \qquad \text{horizontal pair}$$

If $k > n$, these equations (with truncated natural number subtraction) show that both α_{nk} and γ_{nk} are zero, and the identity is trivially true. Otherwise,

$$\begin{aligned}
&(k + 1) \times \alpha_{nk} \times \beta_{nk} \\
&= (n + 2 - (n + 1 - k)) \times \alpha_{nk} \times \beta_{nk} && \text{by } k \leq n \\
&= (n + 2) \times \alpha_{nk} \times \beta_{nk} - (n + 1 - k) \times \alpha_{nk} \times \beta_{nk} && \text{by distribution} \\
&= (n + 1 - k) \times \beta_{nk} \times \beta_{nk} - (n + 1 - k) \times \alpha_{nk} \times \beta_{nk} && \text{by vertical pair} \\
&= (n + 1 - k) \times \beta_{nk} \times \beta_{nk} - (n + 1 - k) \times \beta_{nk} \times \alpha_{nk} && \text{by commutativity} \\
&= (n + 1 - k) \times \beta_{nk} \times (\beta_{nk} - \alpha_{nk}) && \text{by distribution} \\
&= (k + 1) \times \gamma_{nk} \times (\beta_{nk} - \alpha_{nk}) && \text{by horizontal pair}
\end{aligned}$$

Since $k + 1 \neq 0$, the result follows by factor cancellation. □

This identity for a Leibniz triplet is useful in computing the entry γ_{nk} from previously calculated entries α_{nk} and β_{nk}. Indeed, the entire Denominator Triangle can be constructed directly by overlapping triplets:

- Each left boundary entry: $(n + 1)$ for the n-th row, with n starting from 0.
- Each Leibniz triplet: $\gamma_{nk} = \dfrac{\alpha_{nk} \times \beta_{nk}}{\beta_{nk} - \alpha_{nk}}$.

Moreover, this identity is the key for an important property of the Leibniz triplet.

4.1 LCM Exchange

The whole point of introducing Leibniz's Denominator Triangle for the proof of the consecutive LCM lower bound is due to this remarkable property of a Leibniz triplet:

Theorem 12 *In a Leibniz triplet, the vertical and horizontal pairs share the same least common multiple.*

$$\vdash \ \mathsf{lcm}(\beta_{nk}, \alpha_{nk}) = \mathsf{lcm}(\beta_{nk}, \gamma_{nk})$$

recalling that $[\beta_{nk}; \ \alpha_{nk}]$ *is the vertical pair, and* $[\beta_{nk}; \ \gamma_{nk}]$ *the horizontal pair.*

Proof Let $a = \alpha_{nk}$, $b = \beta_{nk}$, and $c = \gamma_{nk}$ form a Leibniz triplet, with b at the corner. If one (or more) of these entries is outside the usual range, the desired LCM exchange is trivially true[5]:

- if $b = 0$, then both $a = 0$ and $c = 0$.
- if $b \neq 0$, but $a = 0$ then $c = 0$, and *vice versa*.

Otherwise, all a, b, and c are nonzero. Note that $ab = c(b - a)$ by Theorem 11. Therefore,[6]

$$\begin{aligned}
&\mathsf{lcm}(b, c) \\
&= bc \div \mathsf{gcd}(b, c) && \text{by definition} \\
&= abc \div (a \times \mathsf{gcd}(b, c)) && \text{introduce factor } a \text{ above and below division} \\
&= bac \div \mathsf{gcd}(ab, ca) && \text{by common factor } a\text{, commutativity} \\
&= bac \div \mathsf{gcd}(c(b - a), ca) && \text{by Leibniz triplet identity (Theorem 11)} \\
&= bac \div (c \times \mathsf{gcd}(b - a, a)) && \text{extract common factor } c \\
&= ba \div \mathsf{gcd}(b, a) && \text{apply GCD subtraction and cancel factor } c \\
&= \mathsf{lcm}(b, a) && \text{by definition.}
\end{aligned}$$

□

[5] For any number n, $\mathsf{lcm}(0, n) = \mathsf{lcm}(n, 0) = 0$.

[6] Here, all fractional forms are integers, as the numerator is divisible by the denominator.

Voilà! The Leibniz triplet, a small L-shape, is thereby shown to be LCM invariant: we can exchange the LCM computation from vertical to horizontal.

Now we can zoom out to the big L-shape (the right-hand side of Fig. 3). Our main result, Theorem 1, will be deduced from a similar LCM invariance of this "enlarged" L-shape involving a column and a row. We shall see that its LCM invariance property is built up from the LCM invariance of various intermediate Leibniz triplets.

5 Paths Through the Denominator Triangle

To capture the notion of the least common multiple of a list of elements, we picture a path composed of entries within the Denominator Triangle. We formalise paths as lists of numbers, without requiring the path to be connected. However, the paths we work with will be connected (refer to Fig. 3) and include:

Definition 13

- ($\mathcal{L}_{\text{down}}\ n$): the list `[1 .. n + 1]`, which happens to be the first $(n + 1)$ elements of the leftmost column of the Denominator Triangle, reading downwards;
- ($\mathcal{L}_{\text{up}}\ n$): the reverse of ($\mathcal{L}_{\text{down}}\ n$), or the leftmost column of the triangle reading upwards; and
- ($\mathcal{L}_{\text{row}}\ n$): the n-th row of the Denominator Triangle, reading from the left to right.

Due to the LCM exchange within a Leibniz triplet (Theorem 12), we can prove the following:

Theorem 14 *In the Denominator Triangle, consider the first element (at the left boundary) of the n-th row. Then the least common multiple of the column of elements above it is equal to the least common multiple of elements along its row.*

$$\vdash\ \mathsf{list\_lcm}\ (\mathcal{L}_{\text{down}}\ n)\ =\ \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ n)$$

The proof is done *via* a kind of zig-zag transformation, see Fig. 5. In the Denominator Triangle, we represent the entries for LCM consideration as a path of black discs, and indicate the Leibniz triplets by discs marked with small gray dots. Recall that, by Theorem 12, the vertical pair of a Leibniz triplet can be swapped with its horizontal pair without affecting the least common multiple.

It takes a little effort to formalise such a transformation. We use the following approach in HOL4.

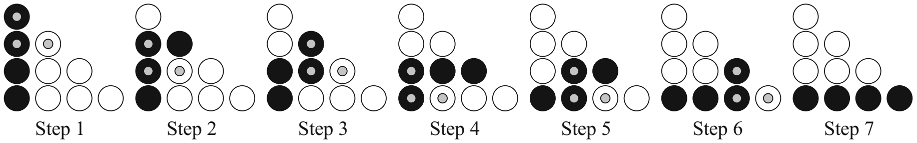

Fig. 5 Transformation of a path from vertical to horizontal in the Denominator Triangle, stepping from left to right. The path is indicated by entries with black discs. The 3 gray-dotted discs in L-shape indicate the Leibniz triplet, which allows LCM exchange. Each step preserves the overall LCM of the path

5.1 Zig-zag Paths

If a path happens to have a vertical pair, we can match the vertical pair with a Leibniz triplet and swap with its horizontal pair to form another path, its zig-zag equivalent, which keeps the overall LCM of the path.

Definition 15 Zig-zag paths are those transformable by a Leibniz triplet.

$$p_1 \leadsto p_2 \iff \exists n\ k\ x\ y.\ p_1 = x \frown [\beta_{nk};\ \alpha_{nk}] \frown y \wedge p_2 = x \frown [\beta_{nk};\ \gamma_{nk}] \frown y$$

Basic properties of zig-zag paths are:

Lemma 16 *Zig-zag path properties.*

$\vdash p_1 \leadsto p_2 \Rightarrow \forall x.\ [x] \frown p_1 \leadsto [x] \frown p_2$ zig-zag is a congruence with respect to $(::)$

$\vdash p_1 \leadsto p_2 \Rightarrow \mathsf{list\_lcm}\ p_1 = \mathsf{list\_lcm}\ p_2$ preserving LCM by exchange *via* triplet

5.2 Wriggle Paths

A path can *wriggle* to another path if there are zig-zag paths in between to facilitate the transformation. Thus:

Definition 17 Wriggling is the reflexive and transitive closure of zig-zagging:

$$p_1 \leadsto^* p_2 = (\leadsto)^*\ p_1\ p_2$$

Lemma 18 *Wriggle path properties.*

$\vdash p_1 \leadsto^* p_2 \Rightarrow \forall x.\ [x] \frown p_1 \leadsto^* [x] \frown p_2$ wriggle is a congruence with respect to $(::)$

$\vdash p_1 \leadsto^* p_2 \Rightarrow \mathsf{list\_lcm}\ p_1 = \mathsf{list\_lcm}\ p_2$ preserving LCM by zig-zags

5.3 Wriggling Induction

We use wriggle paths to establish a key step[7]:

Theorem 19 *In the Denominator Triangle, a left boundary entry with the entire row above it can wriggle to its own row.*

$$\vdash [\mathcal{L}\ (n + 1)\ 0] \frown \mathcal{L}_{\text{row}}\ n \leadsto^* \mathcal{L}_{\text{row}}\ (n + 1)$$

Proof This is a special case of the following general result:

$$\vdash k \leq n + 1 \Rightarrow \mathsf{TAKE}\ (k + 1)\ (\mathcal{L}_{\text{row}}\ (n + 1)) \frown \mathsf{DROP}\ k\ (\mathcal{L}_{\text{row}}\ n) \leadsto^* \mathcal{L}_{\text{row}}\ (n + 1)$$

by putting $k = 0$. Here the list operators TAKE and DROP extract, respectively, prefixes and suffixes of its list. When $k = 0$, $\mathsf{TAKE}\ 1\ (\mathcal{L}_{\text{row}}\ (n + 1)) = [\mathcal{L}\ (n + 1)\ 0]$, and $\mathsf{DROP}\ 0\ (\mathcal{L}_{\text{row}}\ n) = \mathcal{L}_{\text{row}}\ n$.

Note that the path for the general result consists of two parts:

- a lower partial row $p_1 = \mathsf{TAKE}\ (k + 1)\ (\mathcal{L}_{\text{row}}\ (n + 1))$, and
- an upper partial row $p_2 = \mathsf{DROP}\ k\ (\mathcal{L}_{\text{row}}\ n)$.

[7] This is illustrated in Fig. 5 from the middle (Step 4) to the last (Step 7).

The general result is established by induction on the length of the upper partial row p_2, which is $n + 1 - k$.

For the basis, we have $n + 1 - k = 0$, or $k \geq n + 1$ by integer subtraction. Thus $p_1 = \mathcal{L}_{\text{row}}\ (n + 1)$ and $p_2 = [\,]$, with p_1 wriggling to itself.

For the induction step, we have $k < n + 1$, or $k \leq n$. Note that the two-part path can zig-zag to another path with a longer prefix of the lower partial row p_1, and the upper partial row p_2 becomes one entry shorter:

$$\begin{aligned}
&\vdash k \leq n \Rightarrow \\
&\mathsf{TAKE}\ (k + 1)\ (\mathcal{L}_{\text{row}}\ (n + 1)) \frown \mathsf{DROP}\ k\ (\mathcal{L}_{\text{row}}\ n) \leadsto \\
&\mathsf{TAKE}\ (k + 2)\ (\mathcal{L}_{\text{row}}\ (n + 1)) \frown \mathsf{DROP}\ (k + 1)\ (\mathcal{L}_{\text{row}}\ n)
\end{aligned}$$

This is because there is a Leibniz triplet at the zig-zag point (see, for example, Step 5 of Fig. 5), making the zig-zag condition possible. With a shorter p_2, the induction hypothesis applies, and the result follows. □

With this key step, we can prove the whole transformation as illustrated in Fig. 5.

Theorem 20 *For any left boundary entry in the Denominator Triangle, its upward vertical path wriggles to its horizontal path.*

$$\vdash \mathcal{L}_{\text{up}}\ n \leadsto^* \mathcal{L}_{\text{row}}\ n$$

Proof We proceed by induction on n, one less than the length of either $\mathcal{L}_{\text{up}}\ n$ or $\mathcal{L}_{\text{row}}\ n$.

For the basis, $n = 0$, both $\mathcal{L}_{\text{up}}\ 0$ and $\mathcal{L}_{\text{row}}\ 0$ equal to the singleton $[1]$. Hence they wriggle trivially. For the induction step, note that the head of $\mathcal{L}_{\text{up}}\ (n + 1)$ is $\mathcal{L}\ (n + 1)\ 0$. Then,

$$\begin{aligned}
&\mathcal{L}_{\text{up}}\ (n + 1) \\
&\quad = [\mathcal{L}\ (n + 1)\ 0] \frown \mathcal{L}_{\text{up}}\ n && \text{by taking apart head and tail} \\
&\quad \leadsto^* [\mathcal{L}\ (n + 1)\ 0] \frown \mathcal{L}_{\text{row}}\ n && \text{by induction hypothesis and tail wriggle (Lemma 18)} \\
&\quad \leadsto^* \mathcal{L}_{\text{row}}\ (n + 1) && \text{by key step of wriggling (Theorem 19).}
\end{aligned}$$

□

Now we can formally prove the LCM transform: **Theorem** 14

$$\vdash \mathsf{list\_lcm}\ (\mathcal{L}_{\text{down}}\ n) = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ n)$$

Proof Applying path wriggling of Theorem 20 in the last step,

$$\begin{aligned}
&\mathsf{list\_lcm}\ (\mathcal{L}_{\text{down}}\ n) \\
&\quad = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{up}}\ n) && \text{by reverse paths keeping LCM (Lemma 6)} \\
&\quad = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ n) && \text{by wriggle paths keeping LCM (Lemma 18).}
\end{aligned}$$

□

6 LCM Lower Bound

Using the equality of least common multiples in Theorem 14, here is the proof our first key result: **Theorem** 1

$$\vdash 2^n \leq \mathsf{list\_lcm}\ [1 .. n + 1]$$

Proof

$$\begin{array}{ll}
\mathsf{list\_lcm}\ [1\ ..\ n+1] & \\
\quad = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{down}}\ n) & \text{by Definition 13} \\
\quad = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ n) & \text{by LCM transform (Theorem 14)} \\
\quad \geq \lfloor \mathsf{SUM}\ (\mathcal{L}_{\text{row}}\ n) \div \mathsf{LENGTH}\ (\mathcal{L}_{\text{row}}\ n) \rfloor & \text{by average lower bound (Theorem 7)} \\
\quad = 2^n & \text{by denominator row average (Theorem 10)}
\end{array}$$

□

6.1 A Better Lower Bound

Theorem 1 establishes that $2^n \leq \mathsf{list\_lcm}\ [1\ ..\ n+1]$. This lower bound be improved by a simple twist.

Note that Theorem 7 uses the average value of a list of numbers to give a lower bound. This is by addition. Perhaps we can get a tighter bound by multiplication. To this end, we need another simple observation:

Theorem 21 *For a list of positive numbers, its overall* LCM *is bounded below by the least common multiple of any two members (identical or not).*

$$\vdash\ \mathsf{POSITIVE}\ \ell\ \wedge\ \mathsf{MEM}\ x\ \ell\ \wedge\ \mathsf{MEM}\ y\ \ell\ \Rightarrow\ \mathsf{lcm}(x, y)\ \leq\ \mathsf{list\_lcm}\ \ell$$

Proof Let $m = \mathsf{list\_lcm}\ \ell$, a common multiple of all the members in the list ℓ. Thus both x and y divide m, and their least common multiple $\mathsf{lcm}(x, y)$ also divides m. The result follows since $m \neq 0$. □

Observing the symmetry in Figs. 1 and 3, we can see that:

Lemma 22 *Both Pascal's and Leibniz's triangles have symmetrical rows.*

$$\begin{array}{ll}
\vdash\ k \leq n \Rightarrow \binom{n}{k} = \binom{n}{n-k} & \vdash\ k < \lfloor n/2 \rfloor \Rightarrow \binom{n}{k} < \binom{n}{k+1} \\
\vdash\ k \leq n \Rightarrow \mathcal{L}\ n\ k = \mathcal{L}\ n\ (n-k) & \vdash\ k < \lfloor n/2 \rfloor \Rightarrow \mathcal{L}\ n\ k < \mathcal{L}\, n\, (k+1)
\end{array}$$

Note that the central member is unique for a row with an odd number of entries, e.g., the $\mathcal{L}_{\text{row}}\ (2n)$ has $(2n+1)$ entries. We shall pick $x = \mathcal{L}\ (2n)\ n$ and $y = \mathcal{L}\ (2n)\ (n+1)$ to apply Theorem 21.

First, we need a lower bound for x at the middle:

Theorem 23 *A lower bound for the central member of the* $(2n)$*-th row in the Denominator Triangle.*

$$\vdash\ 4^n \leq \mathcal{L}\ (2n)\ n$$

Proof Let $m = 2n$. Note that $\binom{m}{n}$ is the largest in $\mathcal{P}_{\text{row}}\ m$. Using Definition 9 and Theorem 8,

$$\mathcal{L}\ m\ n = (m+1) \times \binom{m}{n} = \sum_{k=0}^{m} \binom{m}{n} \geq \sum_{k=0}^{m} \binom{m}{k} = 2^m = 2^{2n} = 4^n$$

□

We also need the following:

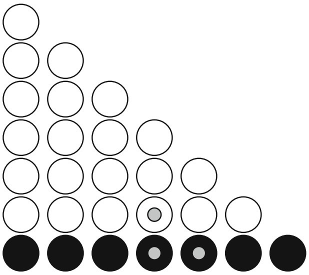

Fig. 6 A lower bound for $L(n)$ by the LCM of a pair of entries. The two entries, situated in a horizontal row (marked by black discs) of the Denominator Triangle, are part of a Leibniz triplet indicated by 3 gray dots

Theorem 24 *An explicit expression for the entry immediately above an entry in the Denominator Triangle.*

$$\vdash 0 < n \Rightarrow \forall k.\ \mathcal{L}\ (n - 1)\ k = (n - k) \times \binom{n}{k}$$

Proof If $k \geq n$, then $n - k = 0$ by integer subtraction. This also means that $k > n - 1$, therefore $\mathcal{L}\ (n - 1)\ k = 0$, and the equality is trivial. Otherwise,

$$\begin{aligned}
&\mathcal{L}\ (n - 1)\ k \\
&\quad = n \times \binom{n - 1}{k} && \text{by Leibniz triangle entry (Definition 9)} \\
&\quad = n \times \frac{(n - 1)!}{k! \times (n - 1 - k)!} && \text{by binomial formula} \\
&\quad = \frac{n!}{k! \times (n - 1 - k)!} && \text{by composing } n! \\
&\quad = (n - k) \times \frac{n!}{k! \times (n - k)!} && \text{by composing } (n - k)! \\
&\quad = (n - k) \times \binom{n}{k} && \text{by binomial formula}
\end{aligned}$$

□

These theorems combine to give the following result due to Nair [18], based on Fig. 6.

Theorem 25 *A lower bound for the consecutive* LCM *up to an odd number.*

$$\vdash n \times 4^n \leq \mathsf{list\_lcm}\ [1\ ..\ 2n + 1]$$

Proof The case $n = 0$ is trivial, so we assume $n \neq 0$. Let $m = 2n$, then $n \leq m$ and $n + 1 \leq m$. Note that $\mathcal{L}_{\text{row}}\ m$ is a positive list, with two members $b = \mathcal{L}\ m\ n$ and $c = \mathcal{L}\ m\ (n + 1)$ near the middle. Adding entry $a = \mathcal{L}\ (m - 1)\ n$ above entry b, the entries a, b and c form a Leibniz triplet. Therefore,

$$\begin{aligned}
&\mathsf{list\_lcm}\ [1\ ..\ m + 1] \\
&\quad = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ m) && \text{by LCM transform (Theorem 14)} \\
&\quad \geq \mathsf{lcm}(b, c) && \text{by LCM pair lower bound(Theorem 21)} \\
&\quad = \mathsf{lcm}(b, a) && \text{by LCM exchange for triplet(Theorem 12)}
\end{aligned}$$

To estimate $\mathsf{lcm}(b, a)$, note that $\mathsf{gcd}(n, m + 1) = \mathsf{gcd}(n, 2n + 1) = 1$ by the Euclidean algorithm. Hence,

$$\begin{aligned}
&\mathsf{lcm}(b, a) && \\
&\quad = \mathsf{lcm}(\mathcal{L}\ m\ n, \mathcal{L}\ (m - 1)\ n) && \text{by notation, entry } a \text{ above entry } b \text{ at middle} \\
&\quad = \mathsf{lcm}((m + 1) \times \binom{m}{n}, \mathcal{L}\ (m - 1)\ n) && \text{by Leibniz entry (Definition 9)} \\
&\quad = \mathsf{lcm}((m + 1) \times \binom{m}{n}, (m - n) \times \binom{m}{n}) && \text{by Leibniz up entry (Theorem 24)} \\
&\quad = \mathsf{lcm}(n \times \binom{m}{n}, (m + 1) \times \binom{m}{n}) && \text{by LCM symmetry,} \\
& && m - n = 2n - n = n \\
&\quad = \mathsf{lcm}(n, m + 1) \times \binom{m}{n} && \text{by LCM common factor} \\
&\quad = n \times (m + 1) \times \binom{m}{n} && \text{by LCM of coprimes} \\
&\quad = n \times \mathcal{L}\ m\ n && \text{by Leibniz entry (Definition 9)} \\
&\quad \geq n \times 4^n && \text{by Leibniz central lower bound} \\
& && \text{(Theorem 23).}
\end{aligned}$$

□

Converting this remarkable lower bound for odd values to cover all values is just a few more steps: **Theorem** 2

$$\vdash\ 7 \leq n \Rightarrow 2^n \leq \mathsf{list\_lcm}\ [1\ ..\ n]$$

Proof In fact, we shall prove a stronger version that implies the above assertion:

$$\vdash\ 2^n \leq \mathsf{list\_lcm}\ [1\ ..\ n] \iff n = 0 \lor n = 5 \lor 7 \leq n$$

Let $L(n) = \mathsf{list\_lcm}\ \texttt{[1 .. }n\texttt{]}$, the consecutive LCM function. Assume n is odd, then $n = 2k + 1$ for some k. Applying Theorem 25, $L(2k + 1) \geq k \times 4^k = k \times 2^{2k}$. This can be bounded by $2 \times 2^{2k} = 2^n$ if $k \geq 2$, or $n \geq 5$. Checking Table 1 shows that $n \geq 5$ is indeed optimal for odd n.

Otherwise, n is even. The case $n = 0$ is trivial. Let $n = 2k + 2$ for some k for a nonzero even n. Note that $L(n)$ is monotonic, thus $L(n) = L(2k + 2) \geq L(2k + 1) \geq k \times 4^k = k \times 2^{2k}$ by Theorem 25. This can be bounded by $4 \times 2^{2k} = 2^n$ if $k \geq 4$, or $n \geq 10$. This lower bound also holds for $n = 8$, but fails for nonzero even $n < 8$, as shown in Table 1. Thus $n \geq 8$ is optimal for nonzero even n.

Therefore the only exceptions to $2^n \leq \mathsf{list\_lcm}\ \texttt{[1 .. }n\texttt{]}$ are: $n = 1, 2, 3, 4$, and 6. □

7 LCM Upper Bound

To find an upper bound for $L(n)$, the consecutive LCM up to n, we need another simple observation:

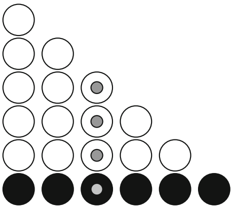

Fig. 7 The Leibniz stack (marked with gray dots) of a base entry lying in a row (marked with black discs) in the Denominator Triangle

Theorem 26 *The* list_lcm *of a list cannot exceed any nonzero common multiple of its members.*

$$\vdash\ 0 < m \wedge (\forall x.\ \mathsf{MEM}\ x\ \ell \Rightarrow x \mid m) \Rightarrow \mathsf{list\_lcm}\ \ell \le m$$

Proof Since list_lcm ℓ is the least common multiple by Lemma 5, it divides any common multiple. □

Thus to give an upper bound of $L(n)$, one way is to find a common multiple of some list whose list_lcm coincides with $L(n)$. Using paths through Leibniz's Denominator Triangle (see Sect. 5), we have the LCM transform of Theorem 14, with $L(n) = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ (n-1))$ for $0 < n$. Therefore, we shall look for a common multiple of all entries along a row in the Denominator Triangle. To achieve this goal, we shall employ a trick distilled from Nair [18], adapted to the Denominator Triangle.

7.1 Leibniz Stacks

Recall from Sect. 6.1 that to obtain a better lower bound for $L(n)$, we focus on a particular row in the Denominator Triangle. We first pick two entries b and c, next to each other, but end up working with a and b where a is above b. How about taking all the entries above b?

Definition 27 Refer to Fig. 7. In the Denominator Triangle, fix an entry $\mathcal{L}\ n\ k$ with $k \le n$. Consider its vertical entries, up to the boundary entry $\mathcal{L}\ k\ k$. All these vertical entries $\mathcal{L}\ m\ k$, where $k \le m \le n$, form the Leibniz stack of the base entry $\mathcal{L}\ n\ k$.

The Leibniz stack for the tip, the top row with $n = 0$, is just itself, called a *trivial* stack. The nontrivial Leibniz stacks for a row with $n \neq 0$ can lead to a common multiple $\mathcal{M}$, by the following strategy:

- *Along a stack* (see Fig. 7):
  - Let $a = \mathcal{L}\ (n-1)\ k$ be the entry immediately above a base entry $b = \mathcal{L}\ n\ k$. In the proof of Theorem 24, we find that $a = (n-k) \times \binom{n}{k}$. But $b = (n+1) \times \binom{n}{k}$ from Definition 9. Therefore $b \mid a \times (n+1)$; i.e., b divides a multiplied with some factor.
  - Similarly, a divides a', the one above it, times another factor, and a' divides a'', the one above it, times yet another factor. Thus, $\mathcal{L}\ m\ k$, an entry on the Leibniz stack with $m \le n$, times a suitable factor f, will be divisible by b, the base entry; i.e., $b \mid \mathcal{L}\ m\ k \times f$.
  - We shall work out what this factor f is in Theorem 29. It turns out that f depends only on n and m, independent of k. This is critical for the next phase.

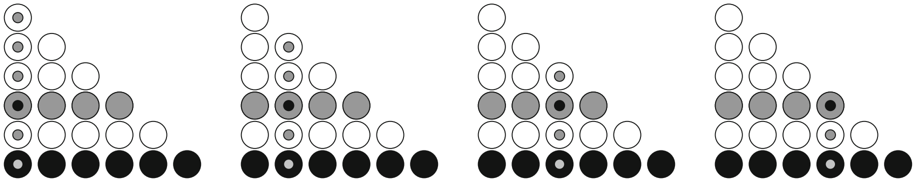

Fig. 8 The Leibniz stacks of entries along a bottom row, with another row above it. Every bottom entry (marked in black) divides a multiple f of its stack entry that intersects the upper row (marked in gray). As a result, f times the list_lcm of the upper row is a common multiple $\mathcal{M}$ for all shadowed entries of the bottom row. If the upper row is at least half as long as the bottom row, $\mathcal{M}$ will be a common multiple for all bottom entries, not just those that are shadowed, by exploiting the symmetry of the Denominator Triangle

- *Across two rows* (see Fig. 8):
  - Let $b_0, b_1, \ldots, b_n$ be the entries along $\mathcal{L}_{\text{row}}\ n$, and $a_0, a_1, \ldots, a_m$ be the entries along $\mathcal{L}_{\text{row}}\ m$, where $m \le n$. That is, $\mathcal{L}_{\text{row}}\ m$ is above $\mathcal{L}_{\text{row}}\ n$ (refer to Fig. 8).
  - Then along the Leibniz stacks, $b_0 \mid a_0 \times f$, and $b_1 \mid a_1 \times f$, all the way across to $b_m \mid a_m \times f$. We will say that entries $b_0 \ldots b_m$ are shadowed by $a_0 \ldots a_m$.
  - Let $e = \text{list\_lcm}\ (\mathcal{L}_{\text{row}}\ m)$. Being a common multiple, $a_0 \mid e$, and $a_1 \mid e$, till $a_m \mid e$. This translates to $a_0 \times f \mid e \times f$, and $a_1 \times f \mid e \times f$, till $a_m \times f \mid e \times f$. In other words, $b_0 \mid e \times f$, and $b_1 \mid e \times f$, until $b_m \mid e \times f$.
  - Thus the product $\mathcal{M} = e \times f$ is a common multiple for b_0, b_1, up to b_m. Note that $m \le n$. Can we make $\mathcal{M}$ a common multiple for all b_0, b_1, up to b_n, so that Theorem 26 applies?
  - If $m \ge \lfloor n/2 \rfloor$, we can exploit the symmetry of the Denominator Triangle to conclude that $\mathcal{M}$ is indeed a common multiple for all entries in $\mathcal{L}_{\text{row}}\ n$. Then Theorem 26 will provide the key to deduce an explicit upper bound for $L(n)$.

Before we can carry out this plan, we need the following:

Theorem 28 *An upper bound for the central binomial coefficient.*

$$\vdash \binom{n}{\lfloor n/2 \rfloor} \le 4^{\lfloor n/2 \rfloor}$$

Proof Let $m = \lfloor n/2 \rfloor$, the integer half of n, and $\mathcal{P}_{\text{row}}\ n$ be the n-th of Pascal's Triangle.

If n is even, then $n = 2m$. Note that $\mathcal{P}_{\text{row}}\ n$ has an odd number of terms, with one central coefficient $\binom{n}{m}$. Since a sum includes all its terms, applying the binomial sum formula of Theorem 8 gives,

$$\binom{n}{m} \le \text{SUM}\ (\mathcal{P}_{\text{row}}\ n) = 2^n = 2^{(2m)} = 4^m$$

Otherwise, n is odd, and $n = 2m + 1$. In this case $\mathcal{P}_{\text{row}}\ n$ has an even number of terms, with two identical central coefficients $\binom{n}{m} = \binom{n}{m + 1}$ by Lemma 22. Again, a sum includes all its terms. Therefore,

$$\binom{n}{m} = \frac{1}{2}\left[\binom{n}{m} + \binom{n}{m + 1}\right] \le \frac{1}{2}\left(\text{SUM}\ (\mathcal{P}_{\text{row}}\ n)\right) = \frac{1}{2}2^n = \frac{1}{2}2^{(2m + 1)} = 4^m$$

□

7.2 A common multiple for a row

Now we are ready to formalise our strategy to find the common multiple $\mathcal{M}$.

Theorem 29 *In the Denominator Triangle, an entry divides a binomial multiple of any entry of its Leibniz stack.*

$$\vdash k \le m \wedge m \le n \Rightarrow \mathcal{L}\ n\ k \mid \mathcal{L}\ m\ k \times \binom{n+1}{m+1}$$

Proof This divisibility result follows from an identity involving both Leibniz's and Pascal's Triangle:

$$\vdash k \le m \wedge m \le n \Rightarrow \mathcal{L}\ n\ k \times \binom{n-k}{m-k} = \mathcal{L}\ m\ k \times \binom{n+1}{m+1}$$

This identity is a consequence of manipulating factorials from the binomial coefficient formula:

$$\begin{aligned}
&\mathcal{L}\ n\ k \times \binom{n-k}{m-k} \\
&= (n+1) \times \binom{n}{k} \times \binom{n-k}{m-k} && \text{by Leibniz triangle entry (Definition 9)} \\
&= (n+1) \times \frac{n!}{k! \times (n-k)!} \times \frac{(n-k)!}{(m-k)! \times (n-m)!} && \text{by binomial formula} \\
&= (n+1) \times \frac{n!}{k!} \times \frac{1}{(m-k)! \times (n-m)!} && \text{by canceling } (n-k)! \\
&= (n+1) \times \frac{n!}{k! \times (m+1)!} \times \frac{(m+1)!}{(m-k)! \times (n-m)!} && \text{by introducing } (m+1)! \\
&= (m+1) \times \frac{(n+1)!}{k! \times (m+1)!} \times \frac{m!}{(m-k)! \times (n-m)!} && \text{by merge and split of factorials} \\
&= (m+1) \times \frac{m!}{k! \times (m-k)!} \times \frac{(n+1)!}{(m+1)! \times (n-m)!} && \text{by rearrangement} \\
&= (m+1) \times \binom{m}{k} \times \binom{n+1}{m+1} && \text{by binomial formula} \\
&= \mathcal{L}\ m\ k \times \binom{n+1}{m+1} && \text{by Leibniz triangle entry (Definition 9)}
\end{aligned}$$

□

As discussed in the strategy (Sect. 7.1), the list_lcm of the upper m-th row, multiplied by the binomial $\binom{n+1}{m+1}$, should be a common multiple $\mathcal{M}$ for all entries of the bottom n-th row, provided that the upper row is not too short. This is because the simple argument only holds for bottom entries that are shadowed by top entries (refer to Fig. 8), with $m \le n$. In order that the extra bottom entries can be covered by symmetry, the upper row must be at least half as long as the bottom row, i.e., $\lfloor (n+1)/2 \rfloor \le (m+1)$, which simplifies to $\lfloor n/2 \rfloor \le m$. This condition can be rewritten as $n \le 2m+1$, which is required in the following:

Theorem 30 *For two rows in the Denominator Triangle, if the upper is at least half as long as the lower, then the* list_lcm *of the upper row multiplied by a binomial factor is a common multiple of all lower entries.*

$$\vdash n \le 2m + 1 \land m \le n \land \mathsf{MEM}\ x\ (\mathcal{L}_{\text{row}}\ n) \Rightarrow$$
$$x \mid \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ m) \times \binom{n+1}{m+1}$$

Proof Note that $m \le n$ puts $\mathcal{L}_{\text{row}}\ m$ as the upper row, and $\mathcal{L}_{\text{row}}\ n$ as the lower row (when $m = n = 0$, they form a "dummy" pair). Denote the common multiple we are after by $\mathcal{M} = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ m) \times \binom{n+1}{m+1}$.

Consider the upper $\mathcal{L}_{\text{row}}\ m$, with entries $y = \mathcal{L}\ m\ k$, for $0 \le k \le m$. Now y divides $\mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ m)$, as the latter is a common multiple. Therefore the product $p = \mathcal{L}\ m\ k \times \binom{n+1}{m+1}$ will divide $\mathcal{M}$.

Next, consider the lower $\mathcal{L}_{\text{row}}\ n$, with entries $x = \mathcal{L}\ n\ k$, where $0 \le k \le n$. If $k \le m$, we can apply Theorem 29 directly, namely x divides the product p. Therefore $x \mid \mathcal{M}$.

Otherwise, $m < k$. Then $n - k \le m$ from the given $n \le 2m + 1$. By symmetry of the Denominator Triangle (Lemma 22), $x = \mathcal{L}\ n\ k = \mathcal{L}\ n\ (n - k)$, which has been shown to divide $\mathcal{M}$. □

7.3 Upper Bound Recurrence

This gives our sought-after common multiple $\mathcal{M}$, enabling us to deduce this result:

Theorem 31 *The consecutive* LCM *function $L(n)$ has a recursive upper bound.*

$$\vdash n \le 2m \land m \le n \Rightarrow L(n) \le L(m) \times \binom{n}{m}$$

Proof If $n = 0$, then $m = 0$, and $L(0) = 1$ and $\binom{0}{0} = 1$, so this case is trivial. Otherwise, $n \ne 0$ and $m \ne 0$. From the given conditions, we have $m - 1 \le n - 1$ and $n - 1 \le 2m - 1 = 2(m - 1) + 1$. Therefore, Theorem 30 applies with n and m replaced by $n - 1$ and $m - 1$. This shows that

$$\mathcal{M} = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ (m - 1)) \times \binom{n}{m}$$

is a common multiple for all entries in $\mathcal{L}_{\text{row}}\ (n - 1)$. By Theorem 26, we have this for a common multiple:

$$\mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ (n - 1)) \le \mathcal{M}$$

But $L(n) = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ (n - 1))$ and $L(m) = \mathsf{list\_lcm}\ (\mathcal{L}_{\text{row}}\ (m - 1))$, by Theorem 14 from the LCM transform in the Denominator triangle (see Sect. 5). The result follows. □

This leads directly to a proof of an upper bound for the consecutive LCM function: **Theorem 3**

$$\vdash L(n) \le 4^n$$

Proof We shall proceed by complete induction on n, with cases for even and odd n.

For the case of even n, let $n = 2m$ for some m. The base case is $n = 0$, which is true since $L(0) = 1$. For the induction step, note that $n \neq 0$ means $m \neq 0$, thus $m < n$. Then, since $n = 2m \leq 2m$,

$$\begin{aligned}
L(n) &\leq L(m) \times \binom{n}{m} && \text{by upper bound recurrence (Theorem 31) using } n \text{ and } m,\\
&\leq 4^m \times \binom{n}{m} && \text{by induction hypothesis, } m < n,\\
&\leq 4^m \times 4^m && \text{by middle binomial coefficient (Theorem 28), } m = \lfloor n/2 \rfloor,\\
&= 4^n && \text{by adding exponents, } n = 2m.
\end{aligned}$$

Therefore $L(n) \leq 4^n$ for even n.

For the case of odd n, let $n = 2m + 1$ for some m. The base case is $n = 1$, which is true since $L(1) = 1$. For the induction step, note that $n \neq 1$ means $m \neq 0$, thus $m + 1 < n$. Also, $n = 2m + 1 < 2(m + 1)$.

$$\begin{aligned}
L(n) &\leq L(m + 1) \times \binom{n}{m + 1} && \text{by upper bound recurrence (Theorem 31)}\\
& && \quad \text{using } n \text{ and } m + 1,\\
&\leq 4^{m + 1} \times \binom{n}{m + 1} && \text{by induction hypothesis, } m + 1 < n,\\
&= 4^{m + 1} \times \binom{n}{m} && \text{by symmetry of binomial coefficients,}\\
& && \quad n - (m + 1) = m,\\
&\leq 4^{m + 1} \times 4^m && \text{by middle binomial coefficient (Theorem 28),}\\
& && \quad m = \lfloor n/2 \rfloor,\\
&= 4^n && \text{by adding exponents, } n = 2m + 1.
\end{aligned}$$

Therefore $L(n) \leq 4^n$ for odd n, too. □

8 Related Work

Our upper bound for the consecutive LCM function $L(n) \leq 4^n$ is not optimal. Hanson [13] established that $L(n) < 3^n$ for $n > 0$, using Sylvester's sequence and estimates of multinomial coefficients. An upper bound for $L(n)$ is not required in our AKS mechanisation work, but it is essential, for example, in the formal proof of the irrationality of $\zeta(3)$ by Frédéric Chyzak *et al.* [8]. Their work assumed, without proof, a slightly weaker upper bound of $L(n)$ than 3^n, but 4^n is too weak for their purpose.

Concerning the central binomial coefficient $B(n) = \binom{2n}{n}$, Theorem 28 gives $B(n) \leq 4^n$. This upper bound is also not optimal. Asperti and Ricciotti [2] proved that $B(n) \leq 4^{n-1}$ for $n > 4$, in their formalization of Chebyshev results in number theory (more on this later).

The growth and bounds of $L(n)$ are depicted in Fig. 9 (compare this to Table 1).

Figure 9 shows evidently that the growth of $L(n)$ is step-wise, and suggests that it can be characterised recursively, starting from $L(0)$ =1:

$$L(n + 1) = \begin{cases} L(n) \times p & \text{if } n + 1 \text{ is a positive power of a prime } p;\\ L(n) & \text{otherwise.} \end{cases}$$

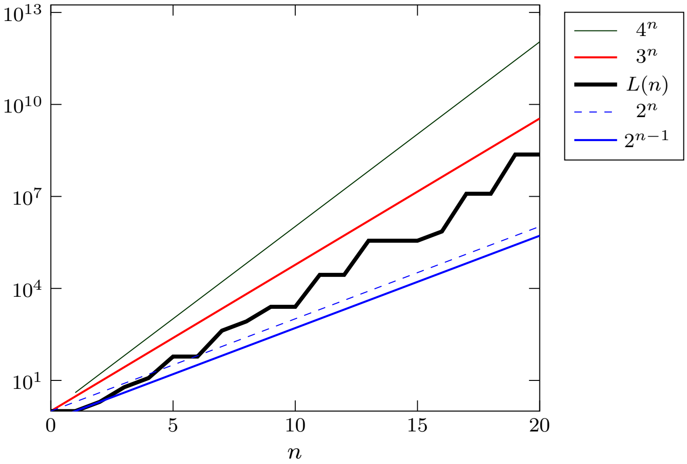

Fig. 9 Comparison of bounds on $L(n)$, the consecutive LCM function

Drawing also on an intuition derived from the von Mangoldt function[8], we hypothesised the recurrence above, tested it on a number of values, and then formalised it.[9] Clearly then, the growth of $L(n)$ is closely related to the distribution of primes.

This distribution is given by the Prime Number Theorem, first conjectured by Legendre and Gauss around 1800, based on tables of primes. For the proof, the first breakthrough came from Chebyshev (1850), who introduced two functions $\theta(n)$ and $\psi(n)$. He showed that the Prime Number Theorem is equivalent to the claim that $\psi(n) \sim n$, which means $\lim_{n\to\infty} \dfrac{\psi(n)}{n} = 1$. He came close, but did not succeed, in getting $\psi(n) \sim n$ (for the full story of the Prime Number Theorem, see Fine and Rosenberger [12]). Hardy and Wright [14] noted that $\psi(n) = \ln L(n)$. Therefore asymptotically $L(n) \sim e^n$ by the Prime Number Theorem (1896) (see Nicolas [19]).

The formalization of Chebyshev's approach was taken up by Asperti and Ricciotti [2]. To avoid working with logarithms, they bounded $\Psi(n) = e^{\psi(n)}$, which is $L(n)$, using upper and lower bounds of the central binomial coefficient $B(n)$. They effectively showed that $2^{\lfloor n/2 \rfloor} \leq L(n) \leq \dfrac{1}{8}(4^n)$. This lower bound on $L(n)$, although weaker than Theorem 1, still suffices to prove our AKS result.

The Prime Number Theorem has been formalised by Avigad *et al.* in Isabelle [3] and independently by John Harrison in HOL Light [15].

9 Conclusion

We have proved both lower and upper bounds for the least common multiple of consecutive numbers, using an interesting application of Leibniz's Triangle in denominator form. By elementary reasoning over natural numbers and lists, we have not just mechanized what we

[8] A "sound wave" which is noisy at prime number times but quiet at other times, as described by Terence Tao [20].

[9] Refer to our proof script primePower for a formalization of this LCM recurrence formula, which requires some effort.

believe to be some cute proofs, but now have a result that will be useful in our ongoing work on the mechanization of the AKS algorithm.

References

1. Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. Ann. Math. **160**(2), 781–793 (2004)
2. Asperti, A., Ricciotti, W.: About the formalization of some results by Chebyshev in number theory. In: *Types for Proofs and Programs, International Conference, TYPES 2008, Torino, Italy, March 26–29, 2008, Revised Selected Papers*, pp. 19–31 (2008)
3. Avigad, J., Donnelly, K., Gray, D., Raff, P.: A formally verified proof of the prime number theorem. ACM Trans. Comput. Logic **9**(1), 2 (2007). doi:10.1145/1297658.1297660
4. Ayoub, A.B.: The harmonic triangle and the beta function. Math. Mag. **60**(4), 223–225 (1987)
5. Bicknell-Johnson, M.: Diagonal sums in the harmonic triangle. Fibonacci Quart. **19**(3), 196–199 (1981)
6. Chan, H.-L., Norrish, M.: Mechanisation of AKS Algorithm: Part 1–the main theorem. In: Urban, C., Zhang, X. (eds.) Interactive Theorem Proving, ITP 2015, Number 9236 in LNCS, pp. 117–136. Springer, Berlin (2015)
7. Chan, H.-L., Norrish, M.: Proof pearl: bounding least common multiples with triangles. In: Blanchette, J.C., Merz, S. (eds.) Interactive Theorem Proving, ITP 2016, Number 9807 in LNCS, pp. 140–150. Springer, Berlin (2016)
8. Chyzak, F., Mahboubi, A., Sibut-Pinote, T., Tassi, E.: A computer-algebra-based formal proof of the irrationality of $\zeta(3)$. In: Klein, G., Gamboa, R. (eds) Interactive Theorem Proving: 5th International Conference, ITP 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14–17, 2014. Proceedings, pp. 160–176. Springer, Cham (2014)
9. Edwards, A.W.F.: Pascal's Arithmetical Triangle: The Story of a Mathematical Idea. Johns Hopkins University Press, Baltimore (2002)
10. Esteve, M.R.M., Delshams, A.: Euler's beta function in Pietro Mengoli's works. Arch. Hist. Exact Sci. **63**(3), 325–356 (2009)
11. Farhi, B.: An identity involving the least common multiple of binomial coefficients and its application. Am. Math. Month. **116**(9), 836–839 (2009)
12. Fine, B., Rosenberger, G.: An epic drama: the development of the prime number theorem. Sci. Ser. A Math. Sci. **20**:1–26 (2010). http://www.mat.utfsm.cl/scientia/
13. Hanson, D.: On the product of the primes. Can. Math. Bull. **15**(1), 33–37 (1972)
14. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 6th edn. Oxford University Press, Oxford (2008). ISBN: 9780199219865
15. Harrison, J.: Formalizing an analytic proof of the Prime Number Theorem (dedicated to Mike Gordon on the occasion of his 60th birthday). J. Autom. Reason. **43**, 243–261 (2009)
16. Hong, S., Nair's, F.: Identities involving the least common multiple of binomial coefficients are equivalent (2009). http://arxiv.org/pdf/0907.3401
17. Grigory, M.: Answer to: Is there a Direct Proof of this LCM identity?. Question 1442 on Math Stack Exchange (2010). http://math.stackexchange.com/questions/1442/
18. Nair, M.: On Chebyshev-type inequalities for primes. Am. Math. Month. **89**(2), 126–129 (1982)
19. Nicolas, A.: Answer to: Reason for LCM of all numbers from $1..n$ equals roughly e^n?. Question 1111334 on Math Stack Exchange (2015). http://math.stackexchange.com/questions/1111334/
20. Tao, T.: Structure and randomness in the prime numbers. A talk delivered at the Science colloquium (2007). https://www.math.ucla.edu/~tao/preprints/Slides/primes.pdf