Divisibility properties of generalized Vandermonde determinants

Stanisław Spież, Jerzy Urbanowicz*
and Paul van Wamelen†

1 Introduction

Given $n \geq 2$ let $\mathbf{a}$ denote an increasing n-tuple of non-negative integers a_i and let $\mathbf{x}$ denote an n-tuple of indeterminates x_i. Denote by $V_{\mathbf{a}}(\mathbf{x})$ the generalized Vandermonde determinant, the polynomial obtained by computing the determinant of the matrix with (i,j) entry equal to $x_i^{a_j}$.

Let $\mathbf{s}$ be the standard n-tuple of consecutive integers from the interval $[0, n-1]$ and given $c \geq 1$ assume that $\mathbf{x}$ is an n-tuple of distinct 2-integral odd rational numbers x_i such that $x_i \equiv x_j \,(\bmod\, 2^{c+1})$.

Several years ago one of the authors, investigating some properties of Kubota-Leopoldt 2-adic L-functions, asked whether for any n-tuples $\mathbf{a}$ and $\mathbf{x}$ with $c = 1$ the identity

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \;=\; \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s}) \tag{1.1}$$

holds. Note that if $n = 2$ and $c = 1$ the above identity is a simple consequence of the well known identity

$$\mathrm{ord}_2(x^a - 1) = \mathrm{ord}_2 a + \mathrm{ord}_2(x-1)\,.$$

*Research of the second author was supported by State Committee for Scientific Research of Poland (KBN) grant 2 P03A 036 15

†Research of the third author was supported by the Louisiana Educational Quality Support Fund grant LEQSF(2000-03)-RD-A-15.

2000 Mathematics Subject Classification: 11C20

Key words and phrases: divisibilities, generalized Vandermonde determinants

In the paper we prove that for any fixed c the identity holds for any $\mathbf{a}$ and $\mathbf{x}$ if the blocks of identical digits of $n-1$ in base 2 are not too large (Theorem 1 and Corollary). Consequentely for any fixed c the identity holds for infinitely many n (Theorem 2). Moreover we prove that for any n identity (1.1) holds for any $\mathbf{a}$ and $\mathbf{x}$ with sufficiently large c (Theorem 4). It means that for sufficiently large c the exponent $\mathrm{ord}_2(V_{\mathbf{a}}(\mathbf{x})/V_{\mathbf{s}}(\mathbf{x}))$ equals $\mathrm{ord}_2(V_{\mathbf{s}}(\mathbf{a})/V_{\mathbf{s}}(\mathbf{s}))$ and so does not depend on $\mathbf{x}$. We also find infinitely many n, $\mathbf{a}$ and $\mathbf{x}$ with $c=1$ such that (1.1) does not hold. More precisely, we proved that for infinitely many n the left hand side of (1.1) is less (resp. greater) than right hand side of (1.1) for some $\mathbf{a}$ and $\mathbf{x}$ (Theorem 3).

A special case of the identity for

$$\mathbf{x}=(1,-7,9,\ldots,2(-1)^{n-1}(2n-1)-1) \text{ or } (-3,5,-11,\ldots,2(-1)^{n}(2n-1)-1),$$

called Wójcik's conjecture, was proved in [4] (cf. [5] and [6]). In this case (1.1) has the form

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) = 3\binom{n}{2} + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a})\,.$$

In the proof the authors made use of some results of this paper. Making use of the above identity they found the so-called full linear congruence for special values of Kubota-Leopoldt 2-adic L-functions $L_2(k,\chi\otimes\omega^{1-k})$ attached to quadratic characters χ with k running over any finite subset of $\mathbb{Z}$ not necessarily consisting of consecutive integers.

1.1 Generalized Vandermonde determinants

The classical Vandermonde determinant $V_{\mathbf{s}}(\mathbf{x})$ is equal to the polynomial

$$\prod_{0\le i<j\le n-1}(x_j-x_i)\,. \tag{1.2}$$

It is well known that the polynomial $V_{\mathbf{a}}(\mathbf{x})$ is divisible by $V_{\mathbf{s}}(\mathbf{x})$ in the polynomial ring $\mathbb{Z}[\mathbf{x}]$ and the quotient $P_{\mathbf{a}}(\mathbf{x}) := V_{\mathbf{a}}(\mathbf{x})/V_{\mathbf{s}}(\mathbf{x})$ is a homogeneous polynomial. The polynomial $P_{\mathbf{a}}(\mathbf{x})$ has exactly $V_{\mathbf{s}}(\mathbf{a})/V_{\mathbf{s}}(\mathbf{s})$ non-negative "terms", i.e., the sum of the coefficients of $P_{\mathbf{a}}(\mathbf{x})$, which all are non-negative, is equal to $V_{\mathbf{s}}(\mathbf{a})/V_{\mathbf{s}}(\mathbf{s})$ (see [1] or [2]). Note that in the $V_{\mathbf{s}}(\mathbf{s})$ we set $0^0=1$.

If $c\in\mathbb{N}$ we define a polynomial $\binom{x}{c}\in\mathbb{Q}[x]$ by $c!\binom{x}{c}=x(x-1)\cdots(x-c+1)$. By definition, set $\binom{x}{0}=1$. $\binom{x}{c}$ is a polynomial of degree c, equal to 0 at integers from the interval $[0,c)$ and equal to 1 at $x=c$.

For n-tuples $\mathbf{a}$ and $\mathbf{x}$ we denote by $C_{\mathbf{a}}(\mathbf{x})$ the polynomial obtained by computing the determinant of the matrix with (i,j) entry equal to $\binom{x_i}{a_j}$. The polynomial $C_{\mathbf{s}}(\mathbf{x})$ is called the Cauchy determinant. We have $C_{\mathbf{s}}(\mathbf{x}) \prod_{i=0}^{n-1} i! = V_{\mathbf{s}}(\mathbf{x})$. Moreover it is well known that the polynomial $C_{\mathbf{a}}(\mathbf{x}) \prod_{i=0}^{n-1} a_i!$ is divisible by $C_{\mathbf{s}}(\mathbf{x}) \prod_{i=0}^{n-1} i!$ in the polynomial ring $\mathbb{Z}[\mathbf{x}]$. Denote by $Q_{\mathbf{a}}(\mathbf{x})$ the quotient of these polynomials.

For $s,\, r \in \mathbb{N}$ and an s-tuple of indeterminates $\mathbf{x}$ denote by $\tau_r(\mathbf{x})$ ($r \leq s$) the elementary symmetric polynomial of degree r. By definition $\tau_0(\mathbf{x}) = 1$ and $\tau_r(\mathbf{x}) = 0$ if $r < 0$. For $r,\, s \in \mathbb{N}$, $r \leq s$ we have

$$\tau_r(\mathbf{x}) = \tau_r(x_1,\, \dots,\, x_{s-1}) + \tau_{r-1}(x_1,\, \dots,\, x_{s-1})x_s \tag{1.3}$$

and these formulas define the elementary symmetric polynomials.

For $t \in \mathbb{N}$, $t \leq s$ and any tuples $\mathbf{x}_1 = (x_{i_1},\, \dots,\, x_{i_t})$, $\mathbf{x}_2 = (x_{i_{t+1}},\, \dots,\, x_{i_s})$ we call the tuples $\mathbf{x}_1$ and $\mathbf{x}_2$ complementary with respect to $\mathbf{x}$ if

$$\{i_1,\, \dots,\, i_t\} \cup \{i_{t+1},\, \dots,\, i_s\} = \{1,\, \dots,\, s\}.$$

By definition, we have

$$\tau_r(-\mathbf{x}) = (-1)^r \tau_r(\mathbf{x})$$

and for $t \leq s$ if $\mathbf{x}_1$ and $\mathbf{x}_2$ are complementary with respect to $\mathbf{x}$ then

$$\tau_r(\mathbf{x}) = \sum_{i=0}^{r} \tau_i(\mathbf{x}_1)\tau_{r-i}(\mathbf{x}_2).$$

Lemma 1 (see [3, Chapter XI, page 334]) *Let* $\mathbf{a}$ (*resp.* $\mathbf{c}$) *be an n-tuple* (*resp. ν-tuple*) *of non-negative integers a_i* (*resp. c_i*) *and let $\mathbf{x}$ be an n-tuple of indeterminates x_i. Assume that* $\mathbf{a}$ *and* $\mathbf{c}$ *are increasing complementary tuples with respect to the standard* $(n+\nu)$*-tuple such that $a_{n-1} = n + \nu - 1$. Then we have*

$$V_{\mathbf{a}}(\mathbf{x}) = \pm V_{\mathbf{s}}(\mathbf{x}) \cdot \det(\tau_{n-c_i+j}(\mathbf{x}))\,,$$

where the row and column indices i and j in the determinant run from 0 to $\nu - 1$.

2 The main theorems

We can now formulate our main results. These results will be proved in subsequent sections. The five presented theorems yield information about identity (1.1). Theorems 2 and 4 follow from the Corollary to Theorem 1. Theorem 3 is a consequence of Lemma 1 and gives infinitely many counter-examples to (1.1). Theorem 5 allows one to make use of computers to verify (1.1) for some fixed n and n-tuples $\mathbf{a}$ in the cases when we cannot use Theorem 1.

Let us consider the expansion of $n-1$ in base 2. A subsequence of this expansion consisting of consecutive 0's or consecutive 1's which is neither preceded nor succeeded by the same symbol we call a block. The number of digits in the block D is said to be its length. The length of D will be denoted by $l(D)$. Set

$$n-1 = D_{2\rho+1}D_{2\rho}\ldots D_1D_0\,,\ \ D_j\text{−blocks},\ \ D_{2\rho+1} = 11\ldots1\,,\ \ D_0 = 00\ldots0$$

and $l(D_j) = l_j$ $(0 \le j \le 2\rho+1)$. Write $p_r = \sum_{s=0}^{r} l_s$ $(0 \le r \le 2\rho+1)$. Assume that the blocks D_j if $1 \le j \le 2\rho+1$ are not empty and in the case when $n-1$ is odd we have $l_0 = 0$ (the block D_0 is empty). For $1 \le k \le \rho$ we define

$$H_k = c\Big(\sum_{j=1}^{k}(2^{p_{2j}} - 2^{p_{2j-1}}) + 2^{p_0}\Big) - \sum_{j=0}^{k} l_{2j+1} \text{ and } H_0 = c2^{l_0} - l_1\,,$$

and

$$H'_k = c\Big(\sum_{j=0}^{k-1}(2^{p_{2j+1}} - 2^{p_{2j}}) + 1\Big) - \sum_{j=0}^{k} l_{2j} \text{ and } H'_0 = c - l_0\,.$$

Theorem 1 *We follow the above notation. Given $n, c \in \mathbb{N}$ $(n \ge 2)$ let $\mathbf{a}$ be an arbitrary increasing n-tuple of non-negative integers and let $\mathbf{x}$ be an n-tuple of distinct 2-integral rational numbers x_i with $x_i \equiv x_j \,(\bmod 2^{c+1})$. Assume that*

$$\min(H_0, H_1, \ldots, H_\rho) \ge 0$$

and

$$\min(c, H_0, H_1, \ldots, H_\rho) + \min(H'_0, H'_1, \ldots, H'_\rho) + 1 \ge 0\,.$$

Then the identity

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \ = \ \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s})$$

holds for $\mathbf{x}$ and $\mathbf{a}$.

Corollary *We follow the notation of Theorem 1. Assume that*

$$l_0 \le c+1\,,\ l_1 \le c2^{l_0}\,,$$

and for $2 \le j \le 2\rho+1$

$$l_j \le c2^{p_{j-2}}(2^{l_{j-1}}-1)\,.$$

Then the identity

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \;=\; \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s})$$

holds for an arbitrary increasing n-tuple $\mathbf{a}$ *of non-negative integers and an arbitrary n-tuple* $\mathbf{x}$ *of distinct 2-integral rational numbers x_i with $x_i \equiv x_j \pmod{2^{c+1}}$.*

Theorem 2 *For any fixed $c \in \mathbb{N}$ there are infinitely many n such that the identity*

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \;=\; \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s})$$

holds for an arbitrary increasing n-tuple $\mathbf{a}$ *of non-negative integers and an arbitrary n-tuple* $\mathbf{x}$ *of distinct 2-integral rational numbers x_i with $x_i \equiv x_j \pmod{2^{c+1}}$.*

Theorem 3 *For any fixed $c \in \mathbb{N}$ there are infinitely many n such the inequality*

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \;>\; \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s})$$

(*resp.*

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \;<\; \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s}))$$

holds for some increasing n-tuple $\mathbf{a}$ *of non-negative integers and some n-tuple* $\mathbf{x}$ *of distinct 2-integral rational numbers x_i with $x_i \equiv x_j \pmod{2^{c+1}}$.*

Theorem 4 *For any $n \in \mathbb{N}$, $n \ge 2$ we can find c_0 such that for all natural numbers $c \ge c_0$ the identity*

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) \;=\; \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s})$$

holds for an arbitrary increasing n-tuple $\mathbf{a}$ *of non-negative integers and an arbitrary n-tuple* $\mathbf{x}$ *of distinct 2-integral rational numbers x_i with $x_i \equiv x_j \pmod{2^{c+1}}$.*

In the sequel let k denote the number of digits in the base 2 expansion of $n-1$. For an increasing n-tuple $\mathbf{a}$ of non-negative integers a_i denote by C^* the subset of the set $[1, a_{n-1}]^{n-1}$ consisting of all increasing $(n-1)$-tuples not equal to $(1, 2, \ldots, n-1)$. Write

$$\gamma = n - 1 + \frac{1}{c}\Big((k-3)\Big(\frac{k-3}{2c} + \sqrt{\Big(\frac{k-3}{2c}\Big)^2 + \frac{2}{c}}\,\Big) + 3\Big)$$

and for $\mathbf{b} \in C^*$ set

$$s := s(\mathbf{b}) = \#\{i \in [1, n-1]\colon\ b_i \geq n\}\,.$$

For $2 \leq r \leq n-2$ let

$$\Gamma_r = \{\mathbf{b} = (b_1, \ldots, b_{n-1}) :\ b_i = i \text{ if } i \leq r-1 \text{ and } r \leq b_r < \ldots < b_{n-1} \leq \gamma\}\,.$$

In the sequel let $s_2(t)$ $(t \in \mathbb{N})$ denote the sum of the digits in the base 2 expansion of t.

Theorem 5 *Given n, $c \in \mathbb{N}$ $(n \geq 2)$ let $\mathbf{a}$ be an increasing n-tuple of non-negative integers a_i and let $\mathbf{x}$ be an n-tuple of distinct 2-integral rational numbers x_i with $x_i \equiv x_j \pmod{2^{c+1}}$. In the notation stated above, identity* (1.1) *holds for $\mathbf{x}$ and $\mathbf{a}$ if the inequality*

$$c\Big(\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i\Big) + \sum_{i=1}^{n-1} s_2(b_i) - \sum_{i=1}^{n-1} s_2(i) > 0 \tag{2.1}$$

holds for all $\mathbf{b} \in \Gamma_r \cap C^*$, with

$$s(\mathbf{b}) \leq \frac{k-3}{2c} + \sqrt{\Big(\frac{k-3}{2c}\Big)^2 + \frac{2}{c}}$$

and r is the smallest integer such that

$$r \geq n - \frac{k+1}{2c} - \Big(\frac{k-3}{2c}\Big)^2 - \frac{1}{4}\,.$$

3 Two auxiliary lemmas

We first prove the main lemma of the paper (Lemma 2). Although the proof of the lemma is rather technical, the lemma allows one to deduce all the results of the paper. It implies Lemma 3, which provides a very useful method for verifying identity (1.1).

Given an n-tuple $\mathbf{x}$ of indeterminates x_i let $\mathbf{x}'$ denote the $(n-1)$-tuple such that $\mathbf{x}$ is a concatenation of x_0 and $\mathbf{x}'$. Let $\tilde{\mathbf{x}} = \mathbf{x} - x_0 \cdot \mathbf{1}$, where $\mathbf{1} = (1, \ldots, 1)$. For n-tuples $\mathbf{x}$ and

$\mathbf{a}$ we shall consider the polynomial $V_{\mathbf{a}'}(\mathbf{x}')$. Again this polynomial is divisible by $V_{\mathbf{s}'}(\mathbf{x}')$ in the polynomial ring $\mathbb{Z}[\mathbf{x}']$. Denote by $P'_{\mathbf{a}'}(\mathbf{x}')$ the quotient of these polynomials. Similarly we denote by $C'_{\mathbf{a}'}(\mathbf{x}')$ the polynomial obtained by computing the determinant of the matrix with (i,j) entry equal to $\binom{x_i}{a_j}$. We have $C'_{\mathbf{s}'}(\mathbf{x}')\prod_{i=1}^{n-1} i! = V_{\mathbf{s}'}(\mathbf{x}')$. Again the polynomial $C'_{\mathbf{a}'}(\mathbf{x}')\prod_{i=1}^{n-1} a_i!$ is divisible in the ring $\mathbb{Z}[\mathbf{x}']$ by the polynomial $C'_{\mathbf{s}'}(\mathbf{x}')\prod_{i=1}^{n-1} i!$ and we denote by $Q'_{\mathbf{a}'}(\mathbf{x}')$ the quotient of these polynomials.

Lemma 2 *Given $n \in \mathbb{N}$ $(n \geq 2)$ let $\mathbf{a}$ be an increasing n-tuple of non-negative integers a_i with $a_0 = 0$ and let $\mathbf{x}$ be an n-tuple of distinct 2-integral rational numbers x_i with $x_0 = 1$ and $x_i \equiv 1 \pmod 4$. If for every $\mathbf{b} \in C^*$*

$$\operatorname{ord}_2\left(\frac{P'_{\mathbf{b}}(\tilde{\mathbf{x}}')\prod_{i=1}^{n-1} i!}{\prod_{i=1}^{n-1} b_i!}\right) \geq 1 \tag{3.1}$$

then for $\mathbf{x}$ and $\mathbf{a}$ identity (1.1) *holds.*

Proof. Our proof starts with the observation that inequality (3.1) implies inequality

$$\operatorname{ord}_2\left(\frac{Q'_{\mathbf{b}}(\mathbf{a}')P'_{\mathbf{b}}(\tilde{\mathbf{x}}')\prod_{i=1}^{n-1} i!}{\prod_{i=1}^{n-1} b_i!}\right) \geq 1\,,$$

which follows from $Q'_{\mathbf{b}}(\mathbf{a}') \in \mathbb{Z}[\mathbf{a}']$. Thus it suffices to prove the lemma under the above assumption.

We first prove that

$$V_{\mathbf{a}}(\mathbf{x}) = \sum_{\mathbf{b}\in C^*\cup\{\mathbf{s}'\}} G(\mathbf{b})\,, \tag{3.2}$$

where

$$G(\mathbf{b}) = \left(\frac{V_{\mathbf{s}}(\mathbf{a})V_{\mathbf{s}}(\mathbf{x})}{V_{\mathbf{s}}(\mathbf{s})}\right)\cdot\left(\frac{Q'_{\mathbf{b}}(\mathbf{a}')P'_{\mathbf{b}}(\tilde{\mathbf{x}}')\prod_{i=1}^{n-1} i!}{\prod_{i=1}^{n-1} b_i!}\right).$$

Subtract in $V_{\mathbf{a}}(\mathbf{x})$ the first row from each of the others and expand by minors on the first column. It follows that

$$V_{\mathbf{a}}(\mathbf{x}) = \det(x_i^{a_j} - 1)\,,$$

where the row and column indices i and j run from 1 to $n-1$. Therefore by definition we obtain

$$V_{\mathbf{a}}(\mathbf{x}) = \sum_{\sigma\in S} \operatorname{sgn}(\sigma) \prod_{i=1}^{n-1} (x_{\sigma(i)}^{a_i} - 1)\,,$$

where S denotes the set of all permutations of the set $\{1, 2, \dots, n\}$. Hence we deduce that

$$V_{\mathbf{a}}(\mathbf{x}) = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{n-1} \Big(\sum_{k=1}^{a_i} \binom{a_i}{k} (x_{\sigma(i)} - 1)^k \Big)\,.$$

Write $A = [1, a_1] \times \cdots \times [1, a_{n-1}]$. The above equation implies

$$V_{\mathbf{a}}(\mathbf{x}) = \sum_{\mathbf{c}\in A} \Big(\prod_{i=1}^{n-1} \binom{a_i}{c_i} \Big) \cdot \Big(\sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{n-1} (x_{\sigma(i)} - 1)^{c_i} \Big) = \sum_{\mathbf{c}\in A} \prod_{i=1}^{n-1} \binom{a_i}{c_i} \cdot \det((x_\mu - 1)^{c_\nu})\,,$$

where $\mathbf{c}$ is an $(n-1)$-tuple of non-negative integers c_i and the row and column indices ν and μ in the determinant run from 1 to $n-1$. Consequently, by virtue of $\binom{a_i}{c_i} = 0$ if $c_i > a_i$, we obtain

$$V_{\mathbf{a}}(\mathbf{x}) = \sum_{\mathbf{c}\in C} F(\mathbf{c})\,, \tag{3.3}$$

where C is the subset of the set $[1, a_{n-1}]^{n-1}$ consisting of all $(n-1)$-tuples of distinct integers c_i and

$$F(\mathbf{c}) = \prod_{i=1}^{n-1} \binom{a_i}{c_i} \cdot \det((x_\mu - 1)^{c_\nu})\,.$$

For $\sigma \in S$ and $\mathbf{c} \in C$ denote by $\mathbf{c}^\sigma$ an n-tuple of $c_{\sigma(i)}$ and let $C(\mathbf{c})$ denote the set consisting of $\mathbf{d} \in C$ such that there exists $\sigma \in S$ satisfying $\mathbf{d} = \mathbf{c}^\sigma$. Set

$$G'(\mathbf{b}) = \sum_{\mathbf{c}\in C(\mathbf{b})} F(\mathbf{c})\,.$$

By virtue of (3.3), we obtain

$$V_{\mathbf{a}}(\mathbf{x}) = \sum_{\mathbf{b}\in C^*\cup\{\mathbf{s}'\}} G'(\mathbf{b})\,. \tag{3.4}$$

Furthermore we have

$$G'(\mathbf{b}) = \sum_{\sigma \in S} \operatorname{sgn}(\sigma) \prod_{i=1}^{n-1} \binom{a_i}{b_{\sigma(i)}} \cdot \det((x_\mu - 1)^{b_\nu}) \,,$$

and so

$$G'(\mathbf{b}) = \det\left(\binom{a_\mu}{b_\nu}\right) \cdot \det((x_\mu - 1)^{b_\nu}) \,,$$

where the row and column indices ν and μ in both the determinants run from 1 to $n-1$.

In other words, we obtain

$$G'(\mathbf{b}) = C_{\mathbf{b}}(\mathbf{a}') \cdot V_{\mathbf{b}}(\tilde{\mathbf{x}}') \,,$$

and so

$$G'(\mathbf{b}) = G(\mathbf{b})$$

because $V_{\mathbf{s}'}(\tilde{\mathbf{x}}') = V_{\mathbf{s}}(\mathbf{x})$ and $V_{\mathbf{s}'}(\mathbf{a}') = V_{\mathbf{s}}(\mathbf{a})$. Hence, by virtue of (3.4), equation (3.2) follows.

Now Lemma 2 follows easily from (3.2). It suffices to observe that

$$G(\mathbf{s}') = \frac{V_{\mathbf{s}}(\mathbf{a}) V_{\mathbf{s}}(\mathbf{x})}{V_{\mathbf{s}}(\mathbf{s})} \,,$$

which is clear from $Q'_{\mathbf{s}'}(\mathbf{a}') = 1$ and $P'_{\mathbf{s}'}(\tilde{\mathbf{x}}') = 1$. ∎

Lemma 3 *Given $n, c \in \mathbb{N}$ $(n \geq 2)$ let $\mathbf{a}$ be an increasing n-tuple of non-negative integers a_i with $a_0 = 0$ and let $\mathbf{x}$ be an n-tuple of distinct 2-integral rational numbers x_i with $x_0 = 1$ and $x_i \equiv 1 \pmod{2^{c+1}}$. We have*

(i) *If for $\mathbf{b} \in C^*$ inequality* (2.1) *holds then inequality* (3.1) *also holds.*

(ii) *Inequality* (2.1) *holds for every $\mathbf{b} \in C^*$ if and only if*

$$c(b - i) + s_2(b) - s_2(i) > 0 \tag{3.5}$$

for every $n \leq b \leq a_{n-1}$ and $1 \leq i \leq n-1$.

Remark Observe that, for $i \leq n-1$ and $b \geq n$, (3.5) holds if either

$$b \geq (n-1) + \frac{k}{c} \text{ or } i \leq n - \frac{k}{c} \,.$$

Proof. (ii) is obvious and we turn to (i). We first notice that $P'_{\mathbf{b}}(\tilde{\mathbf{x}}') \in \mathbb{Z}[\mathbf{x}']$ is a homogeneous polynomial of degree

$$\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i\,.$$

Consequently, by virtue of $x_i \equiv 1 \pmod{2^{c+1}}$, we obtain

$$\operatorname{ord}_2(P'_{\mathbf{b}}(\tilde{\mathbf{x}}')) \geq (c+1)(\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i)\,,$$

which implies (3.1). It remains to make use of the formula $\operatorname{ord}_2(t!) = t - s_2(t)$ $(t \in \mathbb{N})$ and Lemma 3 follows at once. ∎

Remark Note that in Theorems 1, 2, 4 and 5 we may assume without loss of generality that $x_0 = 1$ (i.e. $x_i \equiv 1 \pmod{2^{c+1}}$) and $a_0 = 0$. Indeed, it is easily seen that

$$V_{\mathbf{a}}(\mathbf{x}) = x_0^{(a_0+a_1+\cdots a_{n-1})} V_{\mathbf{a}}(\mathbf{x}x_0^{-1})\,.$$

Consequently, we have

$$V_{\mathbf{a}}(\mathbf{x}) = x_0^{(a_0+a_1+\cdots a_{n-1})} \Big(\prod_{i=1}^{n-1} x_i x_0^{-1}\Big)^{a_0} V_{\tilde{\mathbf{a}}}(\mathbf{x}x_0^{-1}),$$

where $\tilde{\mathbf{a}} = \mathbf{a} - a_0 \cdot \mathbf{1}$. On the other hand we have $V_{\mathbf{s}}(\mathbf{x}) = x_0^{\binom{n}{2}} V_{\mathbf{s}}(\mathbf{x}x_0^{-1})$ and $V_{\mathbf{s}}(\tilde{\mathbf{a}}) = V_{\mathbf{s}}(\mathbf{a})$. Thus it is sufficient to note that the n-tuples $\mathbf{x}x_0^{-1}$ and $\tilde{\mathbf{a}}$ satisfy the restricted assumptions. Consequently, in the proofs of Theorems 1, 2, 4 and 5 we may use Lemmas 2 and 3 which were proved under these assumptions.

4 Proof of Theorem 5

Write

$$B(\mathbf{b}) = c\Big(\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i\Big) + \sum_{i=1}^{n-1} s_2(b_i) - \sum_{i=1}^{n-1} s_2(i)\,.$$

Let $1 \leq r \leq n-1$, $\mathbf{b} \in C^*$ and

$$\mathbf{b} = (b_1,\, b_2,\, \ldots,\, b_{n-1})\,.$$

Write

$$C_r = \{\mathbf{b} \in C^* : \ b_i = i \text{ if } i \le r-1, \ b_r > r\} .$$

Assume that $\mathbf{b} \in C_r$ and recall that $s = s(\mathbf{b})$ denotes the number of $i \in [1, n-1]$ such that $b_i \ge n$. By virtue of

$$\sum_{i=n-s}^{n-1} b_i \ge \sum_{i=0}^{s-1} (n+i) ,$$

we have

$$\sum_{i=r}^{n-1} b_i - \sum_{i=r}^{n-1} i \ge \sum_{i=0}^{s-1} (n+i) - \sum_{i=1}^{s-1} (n-i) - r = 2\sum_{i=1}^{s-1} i + n - r .$$

Consequently, we obtain

$$\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i \ge s(s-1) + n - r .$$

Moreover the left hand side of the above inequality equals $s(s-1)+n-r$ only if

$$\mathbf{b} = (1,\, 2,\, \ldots,\, r-1,\, r+1,\, \ldots,\, n-s,\, n,\, n+1,\, \ldots,\, n+s-1) .$$

Furthermore let us observe that

$$\sum_{i=n-s}^{n-1} b_i \ge \sum_{i=0}^{s-u-1} (n+i) + \sum_{i=0}^{u-1} (n+s+i) ,$$

where u denotes the number of terms of $\mathbf{b}$ exceeding $n+s-1$. Therefore we find that

$$\sum_{i=n-s}^{n-1} b_i \ge \sum_{i=0}^{s-u-1} (n+i) + \sum_{i=s-u}^{s-1} (n+i+u) ,$$

and in consequence

$$\sum_{i=n-s}^{n-1} b_i \ge \sum_{i=0}^{s-1} (n+i) + \sum_{i=s-u}^{s-1} u = \sum_{i=0}^{s-1} (n+i) + u^2 .$$

Thus we obtain

$$\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i \ge s(s-1) + n - r + u^2 . \tag{4.1}$$

Denote by k the number of digits in the base 2 expansion of $n-1$. If $b_{n-1} < 2^{k+1}$ we have $s_2(b_i) \geq 2$ for all $b_i \geq n$ except at most one of them. Thus it follows in this case that

$$\sum_{i=1}^{n-1} s_2(b_i) - \sum_{i=1}^{n-1} s_2(i) \geq 2(s-1) + 1 - (k + (k-1)(s-1)) = -2 - s(k-3) \tag{4.2}$$

because $s_2(i) \leq k$ and $s_2(i) = k$ for at most one of the i's.

Denote by v the number of terms of $\mathbf{b}$ greater than $2^{k+1} - 1$. We see at once that

$$n + s - 1 \leq 2(n-1) \leq 2^{k+1} - 1\,,$$

and so

$$v \leq u\,.$$

Then, by (4.2), we have

$$\sum_{i=1}^{n-1} s_2(b_i) - \sum_{i=1}^{n-1} s_2(i) \geq 2(s-1) + 1 - v(k + (k-1)(s-1)) = -2 - s(k-3) - v\,.$$

Consequently, by virtue of (4.1) and $c \geq 1$, we obtain

$$B(\mathbf{b}) \geq c(s(s-1) + n - r) - 2 - s(k-3)\,,$$

and hence

$$B(\mathbf{b}) \geq c\Big(s^2 - s\Big(1 + \frac{k-3}{c}\Big) + n - r - \frac{2}{c}\Big)\,. \tag{4.3}$$

The above yields (2.1) ($B(\mathbf{b}) > 0$) in the case when $\mathbf{b} \in C_r$ with

$$r < n - \frac{2}{c} - \Big(\frac{k-3+c}{2c}\Big)^2 = n - \frac{k+1}{2c} - \Big(\frac{k-3}{2c}\Big)^2 - \frac{1}{4}\,.$$

In this case the discriminant

$$D = \Big(1 + \frac{k-3}{c}\Big)^2 - 4\Big(n - r - \frac{2}{c}\Big)$$

of the quadratic polynomial

$$s^2 - \Big(1 + \frac{k-3}{c}\Big)s + (n-r) - \frac{2}{c}$$

is negative.

By the definition of s, it follows that

$$s \leq n - r$$

if $\mathbf{b} \in C_r$. Therefore, in view of (4.3), we have

$$B(\mathbf{b}) \geq c\Big(s^2 - s\frac{k-3}{c} - \frac{2}{c}\Big)\,. \tag{4.4}$$

Hence we see that $B(\mathbf{b}) > 0$ if

$$s > \frac{k-3}{2c} + \sqrt{\Big(\frac{k-3}{2c}\Big)^2 + \frac{2}{c}}\,. \tag{4.5}$$

For $\mathbf{b} \in C_r$ let

$$\mathbf{b}' = (b'_1, b'_2, \ldots, b'_{n-1})$$

denote the sequence with

$$b'_i = i \text{ if } i \leq r \text{ and } b'_i = b_{i-1} \text{ if } r+1 \leq i \leq n-1\,.$$

Since

$$\operatorname{card}\{i:\ 1 \leq i \leq n-1,\ b'_i \geq n\} = s - 1\,,$$

by (4.4) we obtain

$$B(\mathbf{b}') \geq c(s-1)^2 - (s-1)(k-3) - 2\,.$$

On the other hand, we have

$$B(\mathbf{b}) - B(\mathbf{b}') = c(b_{n-1} - r) + s_2(b_{n-1}) - s_2(r) \geq c(b_{n-1} - (n-s)) + 1 - (k-1)\,.$$

Consequently, if $s \geq 2$ we obtain

$$B(\mathbf{b}) \geq c((s-1)^2 + b_{n-1} - (n-s)) - s(k-3) - 3\,.$$

The above inequality also holds for $s = 1$ because in this case we have

$$B(\mathbf{b}) = c(b_{n-1} - r) + s_2(b_{n-1}) - s_2(r) \geq c(b_{n-1} - (n-1)) + 1 - k\,.$$

Hence, by virtue of $s \geq 1$, we deduce that

$$B(\mathbf{b}) \geq c(b_{n-1} - (n-1)) - (k-3)s - 3\,.$$

Combining the above with the reverse inequality to (4.5) gives

$$B(\mathbf{b}) \geq c(b_{n-1} - (n-1)) - (k-3)\Big(\frac{k-3}{2c} + \sqrt{\Big(\frac{k-3}{2c}\Big)^2 + \frac{2}{c}}\Big) - 3\,.$$

Thus $B(\mathbf{b}) > 0$ if

$$b_{n-1} > n - 1 + \frac{1}{c}\Big((k-3)\Big(\frac{k-3}{2c} + \sqrt{\Big(\frac{k-3}{2c}\Big)^2 + \frac{2}{c}}\,\Big) + 3\Big)\,,$$

which completes the proof of Theorem 5. ■

5 Proof of Theorem 1

The proof of Theorem 1 is a consequence of the following two lemmas.

Lemma 4 *In the notation before the statement of Theorem 1 we have*

$$\min_{b > n-1} \left(c(b - n + 1) + s_2(b) - s_2(n-1)\right) = \min\left(c, H_0, H_1, \ldots, H_\rho\right) + 1\,.$$

Proof. Observe that

$$n - 1 = \sum_{j=0}^{\rho} \left(2^{p_{2j+1}} - 2^{p_{2j}}\right).$$

For $1 \leq k \leq \rho$ let us define

$$a'_k = \sum_{j=k}^{\rho} \left(2^{p_{2j+1}} - 2^{p_{2j}}\right) \text{ and } a_k = a'_k + 2^{p_{2k-1}}\,.$$

Write

$$a_0 = n,\ a_{\rho+1} = 2^{p_{2\rho+1}} \text{ and } a_{\rho+2} = \infty\,.$$

For $0 \leq k \leq \rho + 1$ and $a_k < b < a_{k+1}$ we have

$$c(b - a_k) + s_2(b) - s_2(a_k) > 0$$

because $c(b - a_k) > 0$ and

$$s_2(b) - s_2(a_k) = s_2(b - a'_k) - s_2(a_k - a'_k) = s_2(b - a'_k) - 1 \geq 0\,.$$

Therefore for $1 \leq k \leq \rho + 1$ we have

$$\min_{a_k \leq b < a_{k+1}} (c(b-n+1)+s_2(b)-s_2(n-1)) = c(a_k-n+1)+s_2(a_k)-s_2(n-1) = H_{k-1}+1\,.$$

If $l_0 > 0$ we have

$$\min_{a_0 \leq b < a_1} (c(b-n+1)+s_2(b)-s_2(n-1)) = c(a_0-n+1)+s_2(a_0)-s_2(n-1) = c+1\,.$$

Observe also that if $l_0 = 0$ then $a_0 = a_1$ and $H_0 \leq c+1$. The lemma follows, since

$$a_0 \leq a_1 < a_2 < \ldots < a_{t+1} < a_{t+2} = \infty\,.$$

■

Lemma 5 *In the notation before the statement of Theorem 1 we have*

$$\min_{0 \leq b < n-1} (c(n-1-b)+s_2(n-1)-s_2(b)) = \min\,(H'_0, H'_1, \ldots, H'_\rho)+1\,.$$

Proof. The lemma follows from Lemma 4 by symmetry (i.e. by interchanging digits 0 and 1 and switching inequalities). ■

Proof of Theorem 1: By Lemmas 4 and 5, the inequality

$$c(b-i)+s_2(b)-s_2(i) > 0$$

holds for all $b > n-1$ and $i \leq n-1$ if and only if both assumptions of Theorem 1 are satisfied. Consequently Theorem 1 follows by Lemma 3(ii). ■

Proof of the Corollary to Theorem 1: The inequalities with j odd, in the hypothesis of the Corollary, imply that $H_k \geq 0$ for all $0 \leq k \leq \rho$. Similarly, the inequalities with j even give $H'_k \geq -1$ for all $0 \leq k \leq \rho$. Consequently, the assumptions of Theorem 1 are satisfied and the Corollary follows. ■

6 Proofs of Theorem 2, 3 and 4

Proof of Theorem 2: We shall define a sequence $(n_\nu)_{\nu\geq 1}$ of distinct natural numbers by induction on ν such that the expansion of $n_\nu - 1$ in base 2 has 2ν blocks $D_{2\nu-1}\ldots D_1 D_0$ and the lengths of these blocks l_0, l_1, …, $l_{2\nu-1}$ satisfy the assumptions of the Corollary to Theorem 1 for the fixed c. Write, by definition, $n_1 = 2$.

The expansion of $n_1 - 1$ in base 2 is $D_1 D_0$, where $D_1 = 1$ and D_0 is empty, so the assumptions of the Corollary to Theorem 1 are satisfied. Let us assume that we have defined n_ν such that the expansion $D_{2\nu-1} \ldots D_1 D_0$ of $n_\nu - 1$ in base 2 satisfies the assumptions of the Corollary to Theorem 1. Then we define

$$n_{\nu+1} = D_{2\nu+1} D_{2\nu} \ldots D_1 D_0 + 1\,,$$

where the lengths $l_{2\nu-1}$ and $l_{2\nu}$ satisfy

$$l_{2\nu-1} \leq c 2^{p_{2\nu-3}} (2^{l_{2\nu-2}} - 1) \text{ and } l_{2\nu} \leq c 2^{p_{2\nu-2}} (2^{l_{2\nu-1}} - 1)\,.$$

It is easily seen that the numbers $l_0, l_1, \ldots, l_{2\nu+1}$ satisfy the assumptions of the Corollary to Theorem 1, which gives the theorem. ∎

Proof of Theorem 3: Let $t \geq 1$. Set

$$\mathbf{a} = (0, 1, \ldots, n-t-1, n-t+1, n-t+2, \ldots, n)\,.$$

Then by Lemma 1 we obtain

$$P_{\mathbf{a}}(\mathbf{x}) = \pm \tau_t(\mathbf{x})\,.$$

On the other hand, in this case we have

$$\frac{V_{\mathbf{s}}(\mathbf{a})}{V_{\mathbf{s}}(\mathbf{s})} = \binom{n}{t}\,.$$

Therefore the left hand side of identity (1.1) minus $\mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x})$ takes the form $\mathrm{ord}_2(\tau_t(\mathbf{x}))$ and the right hand side of this identity minus $\mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x})$ equals $\mathrm{ord}_2\binom{n}{t}$. In particular, if $t = 1$ we have

$$\mathbf{a} = (0, 1, \ldots, n-2, n)$$

and the left hand side of (1.1) minus $\mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x})$ takes the form $\mathrm{ord}_2(\tau_1(\mathbf{x}))$ and the right hand side of the equation minus $\mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x})$ is equal to $\mathrm{ord}_2 n$, where $\tau_1(\mathbf{x}) = \sum_{i=0}^{n-1} x_i$.

Set $\tau = \#\{i \in [0, n-1]\colon\ x_i \equiv 1 + 2^{c+1} \pmod{2^{c+2}}\}$. It suffices to consider n and $\mathbf{x}$ satisfying

$$2^{c+1} | n \text{ and } \tau \text{ odd}\,.$$

Indeed, we have

$$\tau_1(\mathbf{x}) \equiv n + \tau 2^{c+1} \pmod{2^{c+2}}\,.$$

Thus if $2^{c+1}||n$ we have

$$\operatorname{ord}_2(\tau_1(\mathbf{x})) \geq c+2\,,$$

and hence for these n the former inequality of Theorem 3 holds. If $2^{c+2}|n$ we have

$$\operatorname{ord}_2(\tau_1(\mathbf{x})) = c+1\,,$$

and hence for these n the latter inequality of Theorem 3 holds. ■

Proof of Theorem 4: Given n it is sufficient to set

$$c_0 = \max\Big(l_0 - 1, \frac{l_1}{2^{l_0}}, \max_{2\leq j\leq l-1}\Big(\frac{l_j}{2^{p_{j-2}}(2^{l_{j-1}}-1)}\Big)\Big)\,.$$

Then the assumptions of the Corollary to Theorem 1 are satisfied for the given n and identity (1.1) holds for any $\mathbf{a}$ and $\mathbf{x}$ with $x_i \equiv x_j \pmod{2^{c+1}}$. ■

7 Examples, Counter-examples and Computations

This section explains how one can compute examples and counter-examples to (1.1) for quite large n.

7.1 Good numbers

In order to simplify the rest of the discussion let us make the following definitions. Let $n, c \in \mathbb{N}$ $(n \geq 2)$. Recall that k denotes the number of digits in the base 2 expansion of $n-1$ and for a given $(n-1)$-tuple $\mathbf{b}$, $s = s(\mathbf{b})$ denotes the number of $i \in [1, n-1]$ such that $b_i \geq n$.

Definition 1 *Fix $n, c \in \mathbb{N}$ $(n \geq 2)$. An increasing $(n-1)$-tuple $\mathbf{b}$ not satisfying inequality* (2.1) *will be called n-suspicious.*

Remark Note that from the proof of Theorem 5 it follows that all n-suspicious sequences $\mathbf{b}$ satisfy

$$s(\mathbf{b}) \leq \frac{k-3}{2c} + \sqrt{\Big(\frac{k-3}{2c}\Big)^2 + \frac{2}{c}}$$

and belong to Γ_r, where r is the smallest integer such that

$$r \geq n - \frac{k+1}{2c} - \Big(\frac{k-3}{2c}\Big)^2 - \frac{1}{4}\,.$$

Observe that for fixed $n, c \in \mathbb{N}$ the number of such sequences is finite.

Definition 2 *Fix* $n, c \in \mathbb{N}$ $(n \geq 2)$. *We say that* n *is good if it satisfies the assumptions of Theorem 1.*

Remark Note that n is good if and only if n satisfies inequality (3.5) for all b and i such that

$$n \leq b < (n-1) + \frac{k}{c} \text{ and } n - \frac{k}{c} < i \leq n-1\,.$$

Moreover, note that by Theorem 1 identity (1.1) holds for all good n. A natural number n not being good is said to be non-good.

By Theorem 5 the only possible counter-examples to (1.1) occur when there are suspicious sequences in C^*. Thus in order to find counter-examples we start with a search for suspicious sequences. We wrote a C program to check each n to first determine whether n is good. If n is non-good we check inequality (2.1) for sequences $\mathbf{b} \in \Gamma_r$, where $s(\mathbf{b})$ and r are the same as in the Remark after Definition 1. In order to speed up this program it is very useful to precompute the s_2 function for arguments a little beyond the biggest n you will be considering.

1. For $c = 2$ this program finds all suspicious sequences up to $n = 10^4$ in about 36 hours. All $4 < n < 10^4$ that are not good are determined by nine arithmetical progressions:

$$n \equiv 0 \,(\bmod 2^3\,), \quad n \equiv \pm 1 \,(\bmod 2^6\,), \quad n \equiv \pm 2 \,(\bmod 2^8\,)\,,$$

$$n \equiv \pm 3 \,(\bmod 2^{11}\,), \quad n \equiv \pm 4 \,(\bmod 2^{12}\,)\,.$$

2. For $c = 1$ the program is much slower. The program could only get up to $n = 2^8$ after 4 days. All non-good $2 < n \leq 2^8$ are determined by seven arithmetical progressions:

$$n \equiv 0 \,(\bmod 2^2\,), \quad n \equiv \pm 1 \,(\bmod 2^4\,)\,,$$

$$n \equiv \pm 2 \,(\bmod 2^5\,) \quad n \equiv \pm 3 \,(\bmod 2^7\,)\,.$$

The number of n-suspicious sequences for $c = 1$ and $n \leq 2^8$ is several times greater than the number of n-suspicious sequences for $c = 2$ and $n < 10^4$.

7.2 Modified Wójcik's sequences

Many counter-examples we know are related to the so-called Wójcik sequences defined in Theorem 6 below and the main motivation for this paper was a conjecture made by A. Wójcik (private communication) several years ago.

Theorem 6 (Wójcik's Conjecture, see [4, Proposition 4]) *For*

$$\mathbf{w} = (w_0,\, w_1,\, \ldots,\, w_{n-1}) \text{ and } \mathbf{v} = (v_0,\, v_1,\, \ldots,\, v_{n-1}),$$

where

$$w_i = 2(-1)^i(2i+1) - 1 \text{ and } v_i = -2(-1)^i(2i+1) - 1 \;(0 \le i \le n-1)$$

and every $\mathbf{a}$ *we have*

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{w}) = \mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{v}) = \; 3\binom{n}{2} + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a})\,.$$

We shall make use of some modifications of the sequences $\mathbf{w}$ and $\mathbf{v}$. For an n-tuple $\mathbf{u} = (u_0,\, u_1,\, \ldots,\, u_{n-1})$ let us define

$$\mathbf{u}(s) = (u_0,\, u_1, \ldots,\, \hat{u}_s,\, \ldots,\, u_{n-1})\,,$$

where the hat means that the sequence $\mathbf{u}(s)$ equals the sequence $\mathbf{u}$ without the one term u_s.

For every n, $\mathbf{a}$ and $0 \le s,\, t \le n-1$ identity (1.1) for the modified Wójcik sequences $\mathbf{w}(s)$ and $\mathbf{v}(s)$ takes the form

$$\mathrm{ord}_2(V_{\mathbf{a}(t)}(\mathbf{w}(s))) \;=\; \mathrm{ord}_2(V_{\mathbf{a}(t)}(\mathbf{v}(s))) \tag{7.1}$$

$$=\; 3\binom{n-1}{2} + \mathrm{ord}_2\Big(\binom{n-1}{[\frac{n+s}{2}]}\Big) + \mathrm{ord}_2\Big(\prod_{\substack{0 \le j < i \le n-1 \\ i,\, j \ne t}} (a_i - a_j)\Big)\,.$$

As was already mentioned Wójcik's conjecture was proved in [4]. We shall show that the above identity is false for some n, $\mathbf{a}$, s and t which gives many counter-examples to identity (1.1).

7.3 Computations with Wójcik's sequences

Knowing non-good n doesn't give us counter-examples, it only shows us where to look for them. We still need to find $\mathbf{a}$ and $\mathbf{x}$ and compare the two sides of (1.1). We therefore need to be able to compute terms of (1.1) for large values of n. This is made possible by Lemma 1 provided that we can compute $\tau_r(\mathbf{x})$ quickly even for large n. This in turn is possible if $\mathbf{x}$ has some simple structure.

If the terms of $\mathbf{x}$ are given in a polynomial form, for instance if $x_i = 4i + 1$, we can use the following technique to compute formulas for $\tau_r(\mathbf{x})$ for moderately sized r (say $r \leq 20$) and any n. We use Mathematica. Its `Sum` function can do symbolic summation, and as $\tau_1(\mathbf{x})$ is just a sum of polynomial terms Mathematica can compute the formula for $\tau_1(\mathbf{x})$ as a polynomial in n.

Now we use the recursive relation (1.3) for $\tau_r(\mathbf{x})$, in the form

$$\tau_r(\mathbf{x}) = \sum_{i=0}^{n-1} x_{n-1-i}\tau_{r-1}(x_0, x_1, \ldots, x_{n-2-i}).$$

If $\tau_{r-1}(\mathbf{x})$ is known as a polynomial in n, this sum is a sum of polynomials and again Mathematica can compute the sum symbolically (it knows the power summation formulas for consecutive integers). As an example the Mathematica code below will compute the formulas for $\tau_r(\mathbf{x})$ in the case were $x_i = 1 + 4i$ for all $r \leq 10$.

```
taurx[r_/; r < 0,n_] := 0;
taurx[0,n_] := 1;

x[i_] := 1+4*i;

taurx[r_,n_] := taurx[r,n_] = Simplify[
  Sum[x[n-1-i]*taurx[r-1,n-1-i],{i,0,n-1}]]

Do[taurx[r,n];Print[taurx[r,n]],{r,1,10}]
```

This will work for `x` any polynomial in i.

We would like to do the above in the case $\mathbf{x} = \mathbf{w}$. Now the terms of $\mathbf{w}$ are not polynomials, but note that w_{2i} is a polynomial in i and w_{2i+1} is also a polynomial in i. This allows us, for each r, to compute $\tau_r(\mathbf{w})$, for $\mathbf{w}$ of length $2i$, as a polynomial in i by a simple modification of the method outlined above. Similarly for $\tau_r(\mathbf{w})$ with $\mathbf{w}$ of length $2i + 1$.

7.4 Counter-examples

We consider the case when $c = 2$. The other cases can be considered in the same way, however for $c = 1$ the program is much slower. We shall look for counter-examples to (1.1) for n-tuples $\mathbf{a}$ and $\mathbf{x}$ with $x_i \equiv x_j (\bmod 2^{c+1})$ of the following form. Given $\nu \in \mathbb{N}$ let $\mathbf{c}$ be a ν-tuple complementary to $\mathbf{a}$ with respect to the standard $(n+\nu)$-tuple. Similarly, given $\mu \in \mathbb{N}$ let $\mathbf{w}$ denote Wójcik's $(n+\mu)$-tuple. Let $\mathbf{j}$ be a μ-tuple being a subsequence of the standard $(n+\mu)$-tuple. Set

$$\mathbf{i} = n \cdot \mathbf{1} - \mathbf{j} \text{ and } \mathbf{d} = n \cdot \mathbf{1} - \mathbf{c}\,.$$

Let $\mathbf{x}$ be a complementary n-tuple to the tuple $\bar{\mathbf{x}} = (w_{j_{\mu-1}}, \ldots, w_{j_1}, w_{j_0})$ with respect to the tuple $\mathbf{w}$.

We will look for counter-examples to (1.1) with $\mathbf{a}$ and $\mathbf{x}$ of the above form where ν and μ are small. Above we have already seen how to evaluate $\tau_r(\mathbf{w})$. We then use this, combined with the following recursive formula, to efficiently evaluate $\tau_r(\mathbf{x})$ for $\mathbf{x}$ of the above form. We have

$$\tau_r(\mathbf{x}) = \tau_r(\mathbf{w}) - \sum_{i=1}^{\mu} \tau_i(\bar{\mathbf{x}})\tau_{r-i}(\mathbf{x})\,.$$

This can be quickly evaluated if μ is small.

To evaluate $\operatorname{ord}_2(V_{\mathbf{s}}(\mathbf{a})/V_{\mathbf{s}}(\mathbf{s}))$, we use the formula

$$\frac{V_{\mathbf{s}}(\mathbf{a})}{V_{\mathbf{s}}(\mathbf{s})} = \frac{\prod_{i=n}^{n+\nu-1} i! \prod_{0 \le k < m \le \nu-1} (c_m - c_k)}{\prod_{k=0}^{\nu-1} c_k! \prod_{k=0}^{\nu-1} (n+\nu-1-c_k)!},$$

which follows from (1.2). This can be quickly evaluated if ν is small.

For each non-good n we looked for examples of tuples $\mathbf{a}$ and $\mathbf{x}$ such that (1.1) does not hold. It turned out that we could find such counter-examples for all non-good $n < 10^4$. It even happened that the form of the first counter-example we found for a given n turned out to also work for other n's satisfying the same congruence condition. We can therefore present our counter-examples very compactly in Table 1. In this table we list, for each congruence giving n, $\mathbf{d}$ and $\mathbf{i}$ which give $\mathbf{a}$ and $\mathbf{x}$ respectively such that (1.1) does not hold.

Note that the first column of Table 1 gives counter-examples to equation (7.1). We looked for and found more counter-examples to this identity. Of course the identity is

Table 1: Counter-examples to (1.1) given by $(\mathbf{d}, \mathbf{i})$ for all non-good $n \in (4, 10^4)$ with $c = 2$

$n \equiv$	$0 \,(\mathrm{mod} 2^3)$	$\pm 1 \,(\mathrm{mod} 2^6)$	$\pm 2 \,(\mathrm{mod} 2^8)$	$\pm 3 \,(\mathrm{mod} 2^{11})$	$\pm 4 \,(\mathrm{mod} 2^{12})$
$\mathbf{d}$	1	$2, 0$	$3, 1, -1$	$4, 2, 0, -2$	$5, 3, 1, -1, -3$
$\mathbf{i}$	2	$1, 2$	$0, 1, 4$	$-1, 0, 3, 4$	$-2, -1, 2, 3, 6$

true for all good n and any $\mathbf{a}$. For the non-good $n < 10^4$ we checked the equation for all $n - 60 \leq s < n$ and all $\mathbf{c}$ such that $\nu < 7$ and $\mathbf{d}$ is a subsequence of $(1, 2, 3, \ldots, 10)$. The counter-examples we found suggested certain patterns. That these patterns do give counter-examples for all s were then checked by getting Mathematica to simplify the corresponding expressions. All known counter-examples to equation (7.1) are presented in Table 2. For each of a number of congruences that n should satisfy, we list $\mathbf{d}$ and $n - s$, which define $\mathbf{a}$ and s. The counter-example is then given by $\mathbf{a}$ and $\mathbf{w}(s)$. All known s are listed but there are other $\mathbf{c}$'s that would also give counter-examples for a given s.

7.5 Concluding remarks

Let $c = 2$. We shall now describe a method for producing large sets of counter-examples to identity (1.1). In this case Theorem 1 describes all $n < 10^4$ for which this identity holds for any $\mathbf{a}$ and $\mathbf{x}$ with $x_i \equiv x_j \,(\mathrm{mod}\ 2^{c+1})$. For every non-good n we used the method to produce a set Φ of $\mathbf{a}$ tuples and a set Ψ of $\mathbf{x}$ tuples such that equation (1.1) does not hold for any $\mathbf{a} \in \Phi$ and any $\mathbf{x} \in \Psi$.

We make use of equation (3.2). As in the proof of Theorem 5, let

$$B(\mathbf{b}) = c\Big(\sum_{i=1}^{n-1} b_i - \sum_{i=1}^{n-1} i\Big) + \sum_{i=1}^{n-1} s_2(b_i) - \sum_{i=1}^{n-1} s_2(i).$$

That is, for a suspicious $\mathbf{b}$ we have $B(\mathbf{b}) < 0$. Let us define a partial order on vectors, by saying $\mathbf{a} < \mathbf{b}$ if and only if $a_i < b_i$ for every i. For every non-good $n < 10^4$ there is an n-suspicious tuple $\mathbf{b}$ that is $<$-smaller than all other suspicious sequences. Let us denote this minimal $\mathbf{b}$ by $\mathbf{b}_n$. For a given non-good n let Ω be the set of $\mathbf{b}$ such that

Table 2: Counter-examples to equation (7.1)

$n \equiv$	$\mathbf{d}$	$n - s$
$0 \pmod{2^3}$	1	even and $\mathrm{ord}_2(n-s) \le \mathrm{ord}_2(n) - 2$
		odd and $\mathrm{ord}_2(n-s-1) \le \mathrm{ord}_2(n) - 2$
$2^7 + 1 \pmod{2^8}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^3}$
$2^8 + 1 \pmod{2^9}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^4}$
$2^9 + 1 \pmod{2^{10}}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^5}$
$2^9 + 2 \pmod{2^{10}}$	$3, 1, -1$	$\equiv 6, 7 \pmod{2^3}$
$2^{10} + 1 \pmod{2^{11}}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^6}$
$2^{10} + 2 \pmod{2^{11}}$	$3, 1, -1$	$\equiv 6, 7, 10, 11, 14, 15 \pmod{2^4}$
$2^{11} + 1 \pmod{2^{12}}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^7}$
$2^{11} + 2 \pmod{2^{12}}$	$3, 1, -1$	$\not\equiv 0, 1, 2, 3, 4, 5, 16, 17, 20, 21 \pmod{2^5}$
$2^{12} + 1 \pmod{2^{13}}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^8}$
$2^{12} + 2 \pmod{2^{13}}$	$3, 1, -1$	$\not\equiv 0, 1, 2, 3, 4, 5, 32, 33, 36, 37 \pmod{2^6}$
$2^{13} + 1 \pmod{2^{14}}$	$2, 0$	$\not\equiv 0, 1, 2, 3 \pmod{2^9}$
$2^{13} + 2 \pmod{2^{14}}$	$3, 1, -1$	$\not\equiv 0, 1, 2, 3, 4, 5, 64, 65, 68, 69 \pmod{2^7}$

$B(\mathbf{b}) \le B(\mathbf{b}_n)$. Let

$$q_n(\mathbf{b}, \mathbf{x}) = \frac{P'_{\mathbf{b}}(\tilde{\mathbf{x}}') \prod_{i=1}^{n-1} i!}{\prod_{i=1}^{n-1} b_i!}.$$

Note that we proved that $\mathrm{ord}_2(q_n(\mathbf{b}, \mathbf{x})) \ge B(\mathbf{b})$ for all $\mathbf{x}$ and $\mathbf{b} \in \Omega$. It turns out that we could always find many $\mathbf{x}$ such that $\mathrm{ord}_2(q_n(\mathbf{b}_n, \mathbf{x})) = B(\mathbf{b}_n)$ and $\mathrm{ord}_2(q_n(\mathbf{b}, \mathbf{x})) > B(\mathbf{b}_n)$. Let the set of such $\mathbf{x}$ be denoted Ψ. If we can find $\mathbf{a}$ such that $\mathrm{ord}_2(Q'_{\mathbf{b}_n}(\mathbf{a}')) = 0$, then it follows from equation (3.2) that (1.1) does not hold for this $\mathbf{a}$ and any $\mathbf{x} \in \Psi$. We don't want to evaluate $Q'_{\mathbf{b}_n}(\mathbf{a}')$ by evaluating the determinant itself. We overcome this problem by noting that for a fixed $\mathbf{x} \in \Psi$ we shall have $\mathrm{ord}_2(Q'_{\mathbf{b}_n}(\mathbf{a}')) = 0$ if and only if

$$\mathrm{ord}_2 V_{\mathbf{a}}(\mathbf{x}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{x}) - \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{a}) + \mathrm{ord}_2 V_{\mathbf{s}}(\mathbf{s}) = B(\mathbf{b}_n).$$

We have already shown how to evaluate the left hand side of this equation quickly. Using this we found many $\mathbf{a}$ satisfying this equation (for some $\mathbf{x} \in \Psi$, and therefore all

$\mathbf{x} \in \Psi$). This gives the set Φ. This method was used to find Ψ with 10 elements and Φ with 10 elements for each non-good $n < 10^4$. That is, 100 counter-examples to (1.1) for each such n.

8 Acknowledgement

The second author thanks Professor J. Browkin for some helpful conversation concerning Lemma 2. Our thanks also go to Professor A. Schinzel for reading an earlier version of the paper and his valuable comments concerning Theorem 5. Thanks are also due to the referee for many constructive suggestions.

References

[1] Evans, R.J. and Isaacs, I.M., *Generalized Vandermonde determinants and roots of unity of prime order*, Proc. Amer. Math. Soc. **58** (1976), 51–54.

[2] Mitchell, O.H., *Note on determinants of powers*, Amer. J. Math. **4** (1881), 341–344.

[3] Muir, T., *A treatise on the theory of determinants*, Dover Publ., New York 1960.

[4] Urbanowicz, J. and van Wamelen, P.B., *Remarks on linear congruence relation for Kubota-Leopoldt 2-adic L-functions*, to appear in J. Number Theory.

[5] Urbanowicz, J. and Williams, K.S., *Congruences for L-functions*, Math. Appl. **551**, Kluwer Acad. Publ., Dordrecht 2000.

[6] Wójcik, A., *Linear congruence relations for 2-adic L-series at integers*, Compositio Math. **111** (1998), 289–304.

Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8
00-956 Warszawa 10, skr. poczt. 21, POLAND
urbanowi@impan.gov.pl
spiez@impan.gov.pl

Department of Mathematics
Louisiana State University
Baton Rouge, Louisiana 70803, U.S.A.
`wamelen@math.lsu.edu`