A NUMBER-THEORETIC CONJECTURE AND ITS IMPLICATION FOR SET THEORY

LORENZ HALBEISEN

Key words: non-repetitive sequences, axiom of choice, combinatorial number theory
2000 Mathematics Subject Classification: **11B50** 03E25 03E05 11B75 11K31

Abstract

For any set S let $\left|\operatorname{seq}^{1\text{-}1}(S)\right|$ denote the cardinality of the set of all finite one-to-one sequences that can be formed from S, and for positive integers a let $\left|a^S\right|$ denote the cardinality of all functions from S to a. Using a result from combinatorial number theory, Halbeisen and Shelah have shown that even in the absence of the axiom of choice, for infinite sets S one always has $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|2^S\right|$ (but nothing more can be proved without the aid of the axiom of choice). Combining stronger number-theoretic results with the combinatorial proof for $a = 2$, it will be shown that for most positive integers a one can prove the inequality $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right|$ without using any form of the axiom of choice. Moreover, it is shown that a very probable number-theoretic conjecture implies that this inequality holds for every positive integer a in any model of set theory.

1. Motivation

It was proved in [3, Theorem 4] that for any set S with more than one element, the cardinality $\left|\operatorname{seq}^{1\text{-}1}(S)\right|$ of the set of all finite one-to-one sequences that can be formed from S can never be equal to the cardinality of the power set of S, denoted by $\left|2^S\right|$. The proof does not make use of any form of the axiom of choice and hence, the result also holds in models of set theory where the axiom of choice fails. Moreover, in the absence of the axiom of choice, $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|2^S\right|$ is all one can prove about the relation between these two cardinalities. In other words, for each of the statements $\left|\operatorname{seq}^{1\text{-}1}(S)\right| < \left|2^S\right|$, $\left|\operatorname{seq}^{1\text{-}1}(S)\right| > \left|2^S\right|$, and $\left|\operatorname{seq}^{1\text{-}1}(S)\right|$ incomparable to $\left|2^S\right|$, there are models of Zermelo-Fraenkel's set theory without the axiom of choice in which the statement is true (*cf.* [4, §9]). However, in the presence of the axiom of choice, for any infinite set S we always have $\left|\operatorname{seq}^{1\text{-}1}(S)\right| < \left|2^S\right|$. Now, it is natural to ask whether the power set of S, which can be identified by the set of all functions from S to 2, can be replaced by a possibly larger set, namely the set of all functions from S to some integer $a > 2$, where $a = \{0, 1, \ldots, a-1\}$. Again, in the presence of the axiom of choice, for any infinite set S and for any integer $a \geq 2$ we have $\left|2^S\right| = \left|a^S\right|$. On the other hand, it is not hard to show that for example in the ordered Mostowski permutation model (*cf.* [4, §7.2]) the infinite set of atoms (or urelements) U satisfies $\left|a^U\right| < \left|b^U\right|$ whenever $a < b$. Moreover, one can even show that in this model we have $\left|\operatorname{seq}^{1\text{-}1}(U)\right| > \left|a^U\right|$ (for each positive integer a), but $\left|\operatorname{seq}^{1\text{-}1}(U)\right| < \left|\bigcup_{a=1}^{\infty} a^U\right|$. Turning back to our problem we may ask if it is provable without the aid of the axiom of choice that for any infinite set S and for every integer $a \geq 2$ we always have $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right|$. The proof in [3] for the case of $a = 2$ uses a purely number-theoretic result which can be generalized to a large class of numbers a and it is very likely that it holds for all integers $a \geq 2$.

The aim of this paper is to state and give evidence for a number-theoretic conjecture which implies that for any infinite set S and for every integer $a \geq 2$, $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right|$.

2. The Shadow of A000522

In the sequel we present some number-theoretic results of a combinatorial integer sequence. The sequence we are interested in has identification number A000522 in *Sloane's On-Line Encyclopedia of Integer Sequences* [5]. For any non-negative integer n, let $n^\star$ be the number of one-to-one sequences (*i.e.*, sequences without repetitions) we can build with n distinct objects. It is not hard to verify that

$$n^\star = \sum_{k=0}^{n} \binom{n}{k} k! = \sum_{j=0}^{n} \frac{n!}{j!}\,,$$

and that for all positive integers n we have $n^\star = \lfloor en! \rfloor$, where $\lfloor x \rfloor$ denotes the integer part of a real number x and e is the Euler number. In particular, $0^\star = 1$ and $n^\star = n \cdot (n-1)^\star + 1$, which implies that

$$n^\star = e \int_1^\infty t^n e^{-t} dt\,.$$

The first few numbers of the integer sequence $n^\star$ are $0^\star = 1$, $1^\star = 2$, $2^\star = 5$, $3^\star = 16$, $4^\star = 65$, $5^\star = 326$, and further we get *e.g.*, $100^\star \approx 2.53687 \cdot 10^{158}$ and $256^\star \approx 2.33179 \cdot 10^{507}$.

Let us now recall some results of [1]: For each positive integer a, an easy calculation modulo a shows that for all non-negative integers n we have $n^\star \equiv (n+a)^\star \mod a$. In particular, if $a \mid n^\star$, then $a \mid (n+a)^\star$.

The **shadow** $d(a)$ of a positive integer a is being defined by stipulating

$$d(a) := |D(a)|\,, \text{ where } D(a) := \left\{n < a : a \mid n^\star\right\}.$$

The shadow $d(a)$ counts the sequence entries $0^\star, 1^\star, 2^\star, \ldots, (a-1)^\star$ which are divisible by a. As an easy consequence we get the following (*cf.* [1, Corollary 11]):

FACT 2.1. If $d(a)$ is the shadow of some positive integer a and $\prod_{i=1}^{j} p_i^{k_i}$ is the prime decomposition of a, then $d(a) = \prod_{i=1}^{j} d(p_i^{k_i})$.

Therefore, the shadow $d(a)$ of any positive integer a is fully determined by its values on the powers of prime numbers. Further we have that for all positive integers a,

all elements $m \in D(a^{k+1})$ must be of the form $m = n + l\, a^k$,

where $n \in D(a^k)$ and $l \in \{0, 1, \ldots, a-1\}$. Hence, we get inductively that if $d(a) = 0$, then $d(a^k) = 0$ for all positive integers k, and a positive integer a with $d(a) = 0$ is called **annihilating**. An integer $a \geq 2$ is annihilating if and only if a is a multiple of some annihilating prime number, and the sequence of annihilating primes starts with 3, 7, 11, 17, 47, 53, 61, 67, 73, 79, 89, 101, 139, 151, 157, 191, 199, ...

What can we say about non-annihilating numbers? For example is it the case that for all positive integers k we have $d(a) = d(a^k)$? To answer this question, let us repeat the calculation carried out in [1, p. 144]. For positive integers a, h, k, l, n, where $h \leq k$ and $a \geq 2$, we have the following:

$$
\begin{aligned}
(n + la^k)^\star &= \sum_{j=0}^{la^k+n} \frac{(l\,a^k + n)!}{j!} \\
&= \sum_{j=0}^{la^k-1} \frac{(l\,a^k + n)!}{j!} + \sum_{j=la^k}^{l\,a^k+n} \frac{(l\,a^k + n)!}{j!} \\
&= \frac{(l\,a^k + n))!}{(l\,a^k - 1)!} (l\,a^k - 1)^\star + \sum_{j=la^k}^{la^k+n} \frac{(l\,a^k + n)!}{j!} \\
&\equiv l\,a^k\, n!\, (l\,a^k - 1)^\star + \sum_{j=la^k}^{la^k+n} \frac{(l\,a^k + n)!}{j!} \mod a^{k+h} \\
&\equiv l\,a^k\, n!\, (l\,a^k - 1)^\star + n^\star + l\,a^k \sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{j!\,i} \mod a^{k+h} \\
&\equiv n^\star + l\,a^k \left(n!\, (l\,a^k - 1)^\star + \sum_{i=1}^{n} \sum_{j=0}^{i-1} \frac{n!}{j!\,i} \right) \mod a^{k+h} \\
&\equiv n^\star + l\,a^k \underbrace{\left(n!\, (a^h - 1)^\star + \sum_{j=0}^{n-1} \frac{n!}{(j+1)!} j^\star \right)}_{=:\, s_{a^h,n}} \mod a^{k+h} \qquad (\clubsuit)
\end{aligned}
$$

As a consequence of ($\clubsuit$) we get that if $a^k \mid n^\star$ and $a^{k+1} \nmid n^\star$ (where $a \geq 2$ and $k \geq 1$), then $a^{k+1} \mid (n + la^k)^\star$ if and only if $(n^\star/a^k) + l\, s_{a,n} \equiv 0 \mod a$. In particular, if a is

prime, $a^k \mid n^\star$, and $s_{a,n} \not\equiv 0 \mod a$, then there is a unique $l \in \{1, \dots, a\}$ such that $a^{k+1} \mid (n + la^k)^\star$. This leads to the following definition:
Let

$$X(a) := \prod_{n \in D(a)} \mathrm{Mod}(s_{a,n}, a)\,,$$

where $\mathrm{Mod}(a, b)$ denotes the reminder of the division of a by b and

$$s_{a,n} := n!\,(a-1)^\star + \sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\, j^\star\,.$$

An integer $a \geq 2$ with $X(a) \neq 0$ is called **regular**, otherwise it is called **irregular**.

Since the empty product is by definition equal to 1, all annihilating numbers are regular. The following fact, which is Lemma 15 and Proposition 16 of [1], gives a connection between the shadow $d(a)$ of an integer $a \geq 2$ and its regularity:

FACT 2.2. (i) An integer $a \geq 2$ is regular if and only if for all positive integers k we have $d(a^k) = d(a)$.
(ii) If $d(a)$ is the shadow of some positive integer a and $\prod_{i=1}^{j} p_i^{k_i}$ is the prime decomposition of a, then

$$d(a) = \prod_{i=1}^{j} d(p_i)\,,$$

provided each prime p_i is regular or one of the primes is annihilating. In particular, an integer $a \geq 2$ is regular if and only if each prime p_i is regular or one of the primes is annihilating.

The smallest irregular prime is 383, and indeed, $d(383) = 3$ but for all $k \geq 2$ we have $d(383^k) = 2$, so, 383^2 is regular. All other primes smaller than *ten millions* are regular. However, motivated by statistical observations it was conjectured in [1, Section 4] that the expected value for the number of irregular primes below some integer n is asymptotically

$$c \cdot \sum_{\substack{p \leq n \\ p \text{ prime}}} \frac{1}{p}\,,$$

where $c \approx 0.9$ is constant. We also like to mention that similar arguments support the conjecture made in [2] that there are infinitely many primes p, such that $2^{p-1} \equiv 1 \mod p^2$. These primes seem to have the same distribution type as irregular primes, which makes them equally hard to find. In the next section we will use similar heuristic arguments to support Conjectures A, B, and C below.

3. Statistical Investigations

3.1. **The random behaviour of $n^\star$ and $D(a)$.** A positive regular integer a is called **1-regular** if $d(a) \leq 1$. Since 1-regular numbers play an important role in Theorem 5.2, let us first investigate the distribution of 1-regular numbers.

As a consequence of Fact 2.2 and (♣) we get the following:

Corollary 3.1. If a^r is regular, $d(a^r) = 1$, $k \geq r$, $a^k \mid n^\star$, and $a^k \mid (n+t)^\star$, then $a^k \mid t$.

Are there many 1-regular numbers? Analyzing random samples indicate that 1-regular numbers are quite frequent, so the answer is "yes". The first ten 1-regular numbers are 2, 3, 4, 6, 7, 8, 9, 11, 12, and 14.

The following table gives the percentage of 1-regular numbers in the interval $[u, w]$:

u	w	percentage
2	100	75.6%
2	1,000	78.9%
2	10,000	81.0%
2	100,000	81.5%
50,000	60,000	83.1%
90,000	100,000	79.3%
100,000	110,000	77.9%
150,000	155,000	75.9%
200,000	205,000	74.2%

A similar picture we get if we consider just the percentage of 1-regular *prime numbers* in the interval $[u, w]$:

u	w	percentage
2	100	72.0%
2	1,000	75.6%
2	10,000	74.2%
2	100,000	73.2%
50,000	60,000	74.54%
90,000	100,000	71.18%
100,000	110,000	75.28%
150,000	155,000	74.46%
200,000	205,000	74.03%

The two preceding tables lead to the following

Observation 1. More than 80% of the positive integers smaller than $100,000$ as well as more than 73% of the prime numbers smaller than $100,000$ are 1-regular. However, it seems that this percentage decreases for larger intervals, but anyway, since the prime numbers 3, 7, 11, and 17 are annihilating, by Fact 2.2 (ii), the percentage can never be smaller than 50.9%.

Recall that by (♣), where $l = h = k = 1$, for any integer $a \geq 2$ we have $(n+a)^\star \equiv (n^\star + a \cdot s_{a,n}) \mod a^2$. Thus, if $a \mid n^\star$ and $a^2 \nmid n^\star$, then $a^2 \mid (n+a)^\star$ if and only if $\mathrm{Mod}(n^\star, a^2)/a + \mathrm{Mod}(s_{a,n}, a) \equiv 0 \mod a$. So, for $a \geq 2$ and $n \in D(a)$ let

$$\varepsilon(a,n) = \frac{\mathrm{Mod}(\tilde{n} + s_{a,n}, a)}{a} \in [0,1)\,,$$

where $\tilde{n} \equiv \mathrm{Mod}(n^\star, a^2)/a$.

For positive integers w let $\nu(w)$ be the set of integers a with $2 \leq a \leq w$ such that $\varepsilon(a,n) = 0$ for some $n \in D(a)$, and let $\Delta(w) := \sum_{a=2}^{w} d(a)$. If we assume that the probability for $a \in \bigcup_{w=2}^{\infty} \nu(w)$ is $d(a)/a$, then, since $\big(\ln(w) - 0.5\big) \approx \sum_{a=2}^{w} 1/a$, for large integers w we would expect that $|\nu(w)|$ is approximately

$$\frac{\Delta(w)}{w} \cdot \big(\ln(w) - 0.5\big) =: N(w)\,.$$

Let us check if this assumption makes sense:

w	$\Delta(w)$	$\lvert\nu(w)\rvert$	$N(w)$
1,000	741	4	4.8
5,000	3,582	6	5.7
10,000	7,140	6	6.2
50,000	35,075	8	7.4
100,000	71,689	8	7.9
500,000	358,063	9	9.0
1,000,000	716,100	10	9.5

Further we have $\nu(1,000,000) = \{2,\ 5,\ 185,\ 460,\ 1520,\ 2521,\ 12974,\ 20683,\ 127430,\ 923663\}$ with $d(2) = 1$, $d(5) = 2$, $d(185) = 6$, $d(460) = 4$, $d(1520) = 4$, $d(2521) = 1$, $d(12974) = 9$, $d(20683) = 9$, $d(127430) = 4$, $d(923663) = 18$.

Observation 2. The preceding table shows that $0.71 < \Delta(w)/w < 0.75$ and that the probability to have $a \mid n^\star$ and $a^2 \mid (n+a)^\star$ is indeed roughly between $0.71/a$ and $0.75/a$.

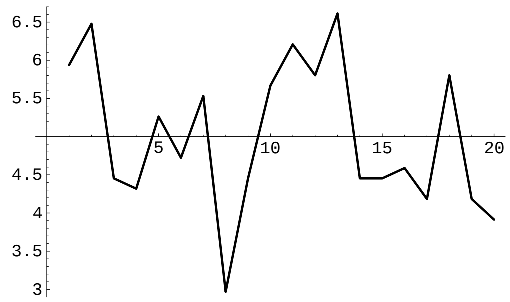
3.2. **More randomness.** Let us now investigate the frequency of integers $a \geq 2$ such that $D(a) \cap D(a^2)$ is non-empty, *i.e.*, $a^2 \mid n^\star$ for some $n \in D(a)$. In order to do so, let us first consider the distribution of the set-function

$$\varphi(a) := \left\{ \frac{(n^\star/a) \mod a}{a} : n \in D(a) \right\} \subseteq [0,1)\,.$$

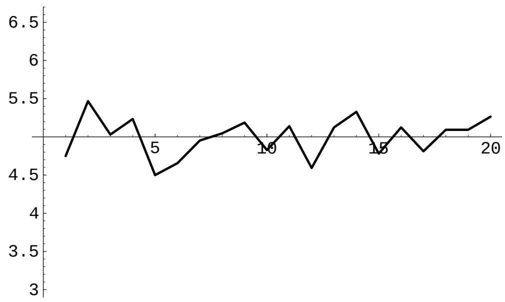
For each of the twenty intervals $I_j = [0.05 \cdot (j-1), 0.05 \cdot j)$, where $1 \leq j \leq 20$, and for a few intervals $[u, w]$, let us compute

$$100 \cdot \frac{\sum_{a=u}^{w} \left|\{r \in \varphi(a) : r \in I_j\}\right|}{\sum_{a=u}^{w} \left|\varphi(a)\right|}\,.$$

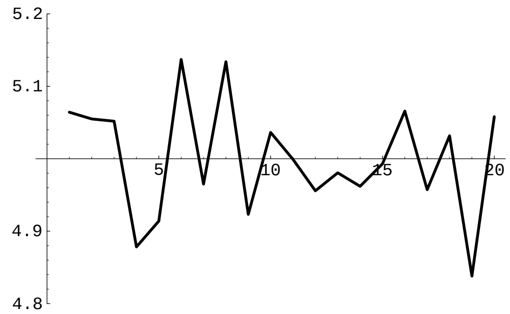
The result of this calculations is shown in the following four graphics:



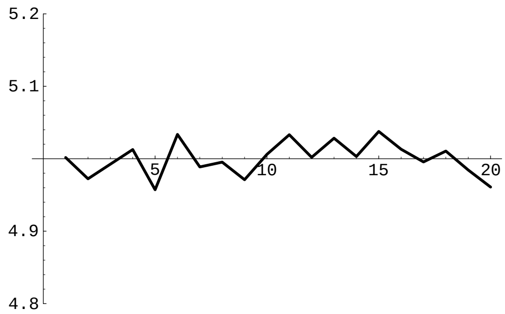
$2 \leq a \leq 1{,}000$



$1{,}000 \leq a \leq 10{,}000$



$10{,}000 \leq a \leq 100{,}000$



$10{,}000 \leq a \leq 1{,}000{,}000$

Observation 3. These four graphics show that for integers $a \leq 1000$, the distribution of φ is far away from being uniform. On the other hand, for integers $a \geq 10000$, the distribution of φ becomes more and more uniform (note the different scales).

For $a \geq 2$, $D(a) \cap D(a^2) \neq \emptyset$ is the same as saying $0 \in \varphi(a)$. Thus, if φ would be uniform, then in the interval $[u, w]$ we would expect to find about

$$\sum_{a=u}^{w} \frac{d(a)}{a} \approx \frac{\Delta(u,w)}{w-u} \sum_{a=w}^{w} \frac{1}{a} \approx \frac{\Delta(u,w)}{w-u} \big(\ln(w) - \ln(u) \big) =: E(u,w)$$

such numbers a, where $\Delta(u,w) = \sum_{a=u}^{w} d(a)$.

Now, let us compare the value of $\frac{3}{4}E(u,w)$ and $2E(u,w)$ with the actual number of such integers a, which is denoted by $\eta(u,w)$:

u	w	$\frac{3}{4}E(u,w)$	$\eta(u,w)$	$2E(u,w)$
1	1,000	3.84	11	10.24
1,000	10,000	1.23	1	3.27
10,000	100,000	1.24	1	3.30
10,000	500,000	2.10	4	5.60
10,000	1,000,000	2.47	5	6.60

The following is the list of pairs (a, n) such that $n \in D(a) \cap D(a^2)$ and $2 \leq a \leq 1,000,000$: $(4, 3)$, $(10, 7)$, $(20, 19)$, $(29, 23)$, $(38, 33)$, $(58, 23)$, $(65, 12)$, $(370, 219)$, $(386, 255)$, $(920, 819)$, $(977, 704)$, $(9727, 2747)$, $(19454, 2747)$, $(170536, 157427)$, $(226735, 153319)$, $(453470, 153319)$, $(788339, 666681)$.

Observation 4. Since $\Delta(u,w)/(w-u)$ is somewhere between 0.71 and 0.75, the preceding table indicates that for large numbers a, the probability to have $D(a) \cap D(a^2) \neq \emptyset$ seems to be somewhere between $1/2a$ and $3/2a$, or roughly about $1/a$.

4. Number-Theoretic Conjectures

In the following we state three number-theoretic conjectures. Conjecture A is the strongest one and states that there are only finitely many positive integers n such that $n^\star = a^k$, where a and k are integers both greater than or equal to 2. Conjecture B, which is motivated by Observation 4, is a weakened version of Conjecture A, but in fact, just Conjecture C, which is the weakest of the three conjectures, will be used later (see Corollary 5.3).

For every integer $a \geq 2$ let

$$P_a = \left\{ n : n^\star = a^k \textit{ for some } k \geq 2 \right\},$$

and let

$$P = \bigcup_{a \geq 2}^{\infty} P_a \,.$$

The only known number in the set P is 16, since $16 = 3^\star$. Even though there is no obvious reason why the set P should be finite, this seems very likely and motivates

CONJECTURE A. The set P is finite.

Let us consider now the set P_a for some integer $a \geq 2$. Let $k_0 \geq 1$ be such that $a^{k_0} > 10^4$ and assume that there exists $k_1 > k_0$ such that $a^{k_1} = n^\star$ for some integer n. Let $k = \lfloor k_1/2 \rfloor$, then, since $n^\star = \lfloor en! \rfloor$, we must have $a^k > n$ which implies that $n \in D(a^k) \cap D\big((a^k)^2\big)$. Now, if we assume—motivated by Observation 4—that the probability for this is roughly $1/a^k$, then, since $\sum_{k=1}^{\infty} 1/a^k$ is finite, this would imply that the set P_a is finite and motivates

CONJECTURE B. For each integer $a \geq 2$, the set P_a is finite.

By Observation 1 it follows that for more than 50% of the integers $a \geq 2$ we have $P_a = \emptyset$. So, Conjecture B is right for more than half of the positive integers. An even weaker conjecture than Conjecture B we get if we just conjecture that for each integer $a \geq 2$, the numbers in P_a become more and more rare.

CONJECTURE C. For each integer $a \geq 2$, the set

$$\big\{n : n^\star = a^k \textit{ for some } k \geq 2 \textit{ and } (n+t) \in P_a \textit{ for some } 1 \leq t \leq k\big\}$$

is finite.

Notice that by Corollary 3.1, Conjecture C is right for all regular integers $a \geq 2$ with $d(a) \leq 1$ (compare with Theorem 5.2). In the next section we will see that if Conjecture C is right, then for any infinite set S and any integer $a \geq 2$, $\big|\operatorname{seq}^{1\text{-}1}(S)\big| \neq \big|a^S\big|$ is provable without using any form of the axiom of choice.

5. A Link to Set Theory

Before we can state the main result of this section we like to explain how to compare the cardinalities of infinite sets in ZF, which is Zermelo-Fraenkel's set theory without the axiom of choice.

For any two sets A and B we say that A has the *same cardinality* as B, denoted by $|A| = |B|$, if there is a bijection between A and B, *i.e.*, a one-to-one function from A onto B. Further, the cardinality of A is *less than or equal to* the cardinality of B, denoted by $|A| \leq |B|$, if $|A| = |B'|$ for some $B' \subseteq B$. If we have neither $|A| \leq |B|$ nor $|B| \leq |A|$, then we say that the cardinalities of the sets A and B are *incomparable*.

Let $\aleph_0$ be the cardinality of the non-negative integers. A set S is called **transfinite** if $\aleph_0 \leq |S|$, *i.e.*, if S contains an infinite one-to-one sequence.

For any set S, let $\operatorname{seq}^{1\text{-}1}(S)$ be the set of all finite one-to-one sequences that can be formed from S, and for any positive integer a, let a^S be the set of all functions from S to $a = \{0, 1, \ldots, a-1\}$. Notice that the set 2^S can be identified with the power set of S.

As it was mentioned before, each of the following statements is consistent with ZF (see [4, §9]):

- $\left|\operatorname{seq}^{1\text{-}1}(S)\right| < \left|2^S\right|$;
- $\left|\operatorname{seq}^{1\text{-}1}(S)\right| > \left|2^S\right|$;
- the cardinalities of the sets $\operatorname{seq}^{1\text{-}1}(S)$ and 2^S are incomparable.

On the other hand, it is provable in ZF that for any set S with more than one element, the cardinality of $\operatorname{seq}^{1\text{-}1}(S)$ is never equal to the cardinality of the power set of S (*cf.* [3, Theorem 4]). The crucial point in the proof of Theorem 4 in [3] was the fact that—in the terminology of the preceding section—the number 2 is regular and $d(2) = 1$. This leads to the following definition:

An integer $a \geq 2$ is called **eventually regular** if there is a positive integer r such that a^r is regular. In view of the fact that there is just one irregular prime known which is even eventually regular, one would expect that all integers $a \geq 2$ are eventually regular. Further, an integer $a \geq 2$ is called **eventually 1-regular** if a^r is regular (for some $r \geq 1$) and $d(a^r) \leq 1$.

In the following we will see that—even in the absence of the axiom of choice—for any eventually 1-regular number $a \geq 2$ and for any infinite set S we always have $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right|$, *i.e.*, there is no bijection between $\operatorname{seq}^{1\text{-}1}(S)$ and a^S. The proof will essentially follow that of Theorem 4 in [3], and the first step is to show that if the infinite set S contains a countable infinite one-to-one sequence, then $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \ngeq \left|a^S\right|$:

LEMMA 5.1 (ZF). Let S be an infinite set. If S is transfinite, then for each integer $a \geq 2$ we have $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \ngeq \left|a^S\right|$.

Proof. In [3, §3] it is shown that if the power set is transfinite, then $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \ngeq \left|2^S\right|$. Firstly, if S is transfinite, then also the power set 2^S is transfinite. Secondly, for any integer $a \geq 2$ we have $\left|2^S\right| \leq \left|a^S\right|$, and Lemma 5.1 follows immediately. ⊣

THEOREM 5.2 (ZF). For any infinite set S, if the integer $a \geq 2$ is eventually 1-regular, then $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right|$.

Proof. By Lemma 5.1 it is enough to prove that if $\left|\operatorname{seq}^{1\text{-}1}(S)\right| = \left|a^S\right|$, then S is transfinite. Thus, towards a contradiction, let us assume that $\left|\operatorname{seq}^{1\text{-}1}(S)\right| = \left|a^S\right|$ and let

$$\begin{array}{rccl} B: & \operatorname{seq}^{1\text{-}1}(S) & \longrightarrow & a^S \\ & \sigma & \longmapsto & f_\sigma : S \to a \end{array}$$

be a bijection between $\operatorname{seq}^{1\text{-}1}(S)$ and a^S. We shall use this bijection to construct an infinite one-to-one sequence $(s_0, s_1, \ldots, s_n \ldots)$ of elements of S. In fact it is enough to show that every finite one-to-one sequence $\sigma_n \in \operatorname{seq}^{1\text{-}1}(S)$ of length n can be extended to a one-to-one sequence $\sigma_n{}^\frown s \in \operatorname{seq}^{1\text{-}1}(S)$ of length $n + 1$.

Since a is eventually 1-regular, there is an $r \geq 2$ so that a^r is regular and $d(a^r) \leq 1$. Pick $a^r + 1$ distinct elements $s_0, s_1, \dots, s_{a^r}$ from S.

Assume that for some $n > a^r$ we already have constructed a one-to-one sequence $\sigma_n = (s_0, s_1, \dots, s_{n-1})$ of elements of S and let $S_n = \{s_i : 0 \leq i < n\}$. The sequence σ_n induces in a natural way an ordering on the set $\mathrm{seq}^{1\text{-}1}(S_n)$, *e.g.*, order $\mathrm{seq}^{1\text{-}1}(S_n)$ by length and lexicographically. Let us define an equivalence relation on S by stipulating

$$x \sim y \iff \forall \sigma \in \mathrm{seq}^{1\text{-}1}(S_n)\big(f_\sigma(x) = f_\sigma(y)\big), \text{ where } f_\sigma = B(\sigma).$$

Let $Eq(n) = S/{\sim}$ be the set of all equivalence classes. The ordering on $\mathrm{seq}^{1\text{-}1}(S_n)$ induces an ordering on $Eq(n)$. Let

$$k = |Eq(n)|,$$

then a^k is equal to the cardinality of the set of functions from $k = \{0, 1, \dots, k-1\}$ to a, where each such function corresponds to a function $Eq(n) \to a$, which again corresponds to a function in a^S. In particular we can identify the set a^k with the cardinality of the set $a^{Eq(n)}$ of all functions $\bar{f} : S \to a$ such that $\bar{f}$ is constant on each member of $Eq(n)$. Now, the ordering on $Eq(n)$ induces in a natural way an ordering on the set of functions $a^{Eq(n)} \subseteq a^S$.

By construction we have $n^\star = |\,\mathrm{seq}^{1\text{-}1}(S_n)| \leq a^k$.

Case 1: If $n^\star < a^k$, then there exists a least (with respect to the ordering on $a^{Eq(n)}$) function $\bar{f}_0 \in a^{Eq(n)}$ such that $\bar{f}_0 \notin \big\{B(\sigma) : \sigma \in \mathrm{seq}^{1\text{-}1}(S_n)\big\}$, which implies that $B^{-1}(\bar{f}_0) \notin \mathrm{seq}^{1\text{-}1}(S_n)$. Let $s_n \in S$ be the first element in the sequence $B^{-1}(\bar{f}_0)$ which does not belong to S_n. Now, $\sigma_n{}^\frown s_n \in \mathrm{seq}^{1\text{-}1}(S)$ is a one-to-one sequence of length $n+1$.

Remark. Notice that if Conjecture B is right, then we can choose n such that for all $m \geq n$, $m \notin P_a$, which implies that we are always in Case 1. In particular, Conjecture B implies that for every infinite set S we have $\big|\mathrm{seq}^{1\text{-}1}(S)\big| \neq \big|a^S\big|$. Further notice that we are always in Case 1 if $d(a) = 0$, which, by Observation 1, holds for more than 50% of the integers $a \geq 2$.

Case 2: Suppose that $n^\star = a^k$. For arbitrary elements $x \in S \setminus S_n$ let us resume the construction with the sequence $\sigma_n{}^\frown x$. By a parity argument one easily sees that $(n+1)^\star$ is not an integer power of a, and thus, we are in Case 1. We proceed as long as we are in Case 1. If there is an element $x \in S \setminus S_n$ such that we are always in Case 1, then we can construct an infinite one-to-one sequence of elements of S and we are done. So, assume that for every $x \in S \setminus S_n$ we get back in Case 2, where we then have the following situation: The one-to-one sequence in S we have constructed is of length $n + \ell + 1$ (for some positive integer ℓ), depends on $x \in S \setminus S_n$, and $(n + \ell + 1)^\star$ is an integer power of a. Let $\sigma^x_{n+\ell} = (s_0, s_1, \dots, s_{n+\ell})$ be this sequence and let $\bar{S}^x = \{s_0, s_1, \dots, s_{n+\ell}\}$. By construction we have $x \in \bar{S}^x$.

*A subset of S is called **good** if it is* not *the union of elements of $Eq(n)$.*

For any set $X \subseteq S$ let $\chi_X : S \to \{0,1\}$ be such that $\chi_X(z) = 1$ iff $z \in X$. Now, for every good set $T \subseteq S$ we have $B^{-1}(\chi_T) \notin \mathrm{seq}^{1\text{-}1}(S_n)$, and therefore, there is a first element in the sequence $B^{-1}(\chi_T)$ which does not belong to the set S_n.

Consider now the set

$$T_{\min} := \{x : \bar{S}^x \textit{ is good and of least cardinality}\}.$$

Since S is infinite, $T_{\min} \neq \emptyset$. If $T_{\min}$ is good, use $B^{-1}(\chi_{T_{\min}})$ to construct a one-to-one sequence in S of length $(n+1)$, and we are done.

Let $m_T := \left|\bar{S}^x\right|$ for some x in $T_{\min}$. For each $x \in T_{\min}$ let us construct a one-to-one sequence SEQ^x in $\bar{S}^x$ of length m_T such that

$$\bar{S}^x = \bar{S}^y \implies \mathrm{SEQ}^x = \mathrm{SEQ}^y .$$

In order to do so, let $x \in T_{\min}$ be arbitrary. Because $\bar{S}^x$ is good,

$$B^{-1}\big(\chi_{\bar{S}^x}\big) \notin \mathrm{seq}^{1\text{-}1}(S_n),$$

and hence there is a first element z in $B^{-1}\big(\chi_{\bar{S}^x}\big)$ which is not in S_n. Resume the construction with $\sigma_n{}^\frown z$ and consider $\bar{S}^z$. It is easy to see that if $\bar{S}^z \subsetneq \bar{S}^x$, then $\bar{S}^z$ is not good (because $x \in T_{\min}$). But then

$$B^{-1}\big(\chi_{\bar{S}^x \setminus \bar{S}^z}\big) \notin \mathrm{seq}^{1\text{-}1}(\bar{S}^z)$$

and we may proceed building the sequence SEQ^x, which depends only on the set $\bar{S}^x$.

For $i < m_T$ define

$$Q_i := \{s \in S : \ s \textit{ is the } i^{th} \textit{ element in } \mathrm{SEQ}^x \textit{ for some } x \in T_{\min}\}.$$

Claim. There is a smallest $j < m_T$ such that Q_j is good.

Then $B^{-1}(\chi_{Q_j}) \notin \mathrm{seq}^{1\text{-}1}(S_n)$, but $B^{-1}(\chi_{Q_j}) \in \mathrm{seq}^{1\text{-}1}(S)$ and we can construct a one-to-one sequence in S of length $n+1$.

It remains to prove the Claim: For any $x \in T_{\min}$ let

$$x^{=} := \{y : \bar{S}^y = \bar{S}^x\},$$

which are the elements of the finite set $\bar{S}^x$ we cannot distinguish, and further let t_0 denote the least cardinality of the sets $x^{=}$, where $x \in T_{\min}$.

Note that if for some $i \neq j$, $z \in Q_i \cap Q_j$, then $\bar{S}^z$ cannot be good (otherwise, SEQ^z would not be unique). Consequently, for each $x \in T_{\min}$ there is exactly one i_x such that $x \in Q_{i_x}$ and for all $y, z \in x^{=}$ with $y \neq z$ we have $i_y \neq i_z$. Hence, if there are no good Q_i's, then t_0 cannot exceed $k = |Eq(n)|$. Let us now show that indeed, t_0 *must* exceed k: Recall that a^r is regular, $d(a^r) \leq 1$, and $n \geq a^r + 1$. Further recall that $n^\star = a^k$ and that $(n+\ell+1)^\star$ is an integer power of a, where $\ell + 1 = m_T - n$. As a consequence of Corollary 3.1, for any positive integer t we get:

$$n^\star = a^k \textit{ and } (n+t)^\star \textit{ is an integer power of } a \textit{ implies } t > k. \qquad (\spadesuit)$$

Take any $x \in T_{\min}$ with $|x^{=}| = t_0$. For any $y \in \bar{S}^x \setminus S_n$, where $\bar{S}^y$ is not necessarily good, we have the following:

- $|\bar{S}^y| = n + t$ where $(n+t)^\star = a^{k'}$ for some $k' > k$, and
- either $y \in x^{=}$ or $\bar{S}^y$ is not good.

Hence, for some non-negative integer t' we have

$$m_T = n + \ell + 1 = n + t' + t_0 = |\bar{S}^x|\,,$$

where $(n+t')^\star$ and $(n+t'+t_0)^\star$ are both integer powers of a. Hence, by ($\spadesuit$), $t_0 > k$ which completes the proof. $\dashv$

As a consequence of the proof of Theorem 5.2 we get the following:

COROLLARY 5.3. If Conjecture C is right, then for any infinite set S and for any integer $a \geq 2$ we always have $\left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right|$, even in the absence of the axiom of choice.

Proof. The crucial point in the proof of Theorem 5.2 was that the assumptions on a^k imply ($\spadesuit$). Now, if Conjecture C is right, then we can choose n_0 such that the set $\big\{n \geq n_0 : n^\star = a^k \textit{ for some } k \geq 2 \textit{ and } (n+t) \in P_a \textit{ for some } 1 \leq t \leq k\big\}$ is empty, which implies ($\spadesuit$). $\dashv$

6. CONCLUSION

Let S be any infinite set and let $a \geq 2$ be an integer. Then we may ask:

$$\text{Is } \left|\operatorname{seq}^{1\text{-}1}(S)\right| \neq \left|a^S\right| \text{ provable in } \mathsf{ZF}\,?$$

In fact, the question just depends on the integer a and therefore it would not be surprising if some number-theoretical arguments are involved in an affirmative answer. Even though it is possible that $\left|2^S\right| \neq \left|a^S\right|$ is provable in ZF without using any number-theoretical results, we do not know of any such proof, not even in the case of $a = 2$.

However, we have seen above that for a large class of numbers a the answer is affirmative: Theorem 5.2 tells us that the answer is “yes” if a is eventually 1-regular and according to the statistics in Section 3.1 and Observation 1, eventually 1-regular numbers are quite frequent.

Further, by the remark in the proof of Theorem 5.2 we see that the answer is also “yes” if Conjecture B is right. Moreover, by Corollary 5.3, even Conjecture C implies that the answer is “yes”. Using some heuristic methods we have seen in Section 4 that Conjecture C is very likely to be right. Thus, if there is a model of ZF in which the equation $\left|2^S\right| = \left|a^S\right|$ holds for some infinite set S and some integer $a \geq 2$, then this number a must be extremely peculiar.

References

[1] Lorenz Halbeisen and Norbert Hungerbühler: *Number theoretic aspects of a combinatorial function*, ***Notes on Number Theory and Discrete Mathematics***, vol. 5 (1999), 138–150.

[2] Lorenz Halbeisen and Norbert Hungerbühler: *On generalized Carmichael numbers*, ***Hardy-Ramanujan Journal***, vol. 22 (1999), 8–22.

[3] Lorenz Halbeisen and Saharon Shelah: *Consequences of arithmetic for set theory*, ***The Journal of Symbolic Logic***, vol. 59 (1994), 30–40.

[4] Lorenz Halbeisen and Saharon Shelah: *Relations between some cardinals in the absence of the axiom of choice*, ***The Bulletin of Symbolic Logic***, vol. 7 (2001), 237–261.

[5] Neil J. A. Sloane: ***The On-Line Encyclopedia of Integer Sequences***, URL Address: http://www.research.att.com/~njas/sequences/

Department of Pure Mathematics, Queen's University Belfast, Belfast BT7 1NN, Northern Ireland, halbeis@qub.ac.uk