

# Universal codes of the natural numbers

Yuval Filmus

July 26, 2013

## Abstract

A code of the natural numbers is a uniquely-decodable binary code of the natural numbers with non-decreasing codeword lengths, which satisfies Kraft's inequality tightly. We define a natural partial order on the set of codes, and show how to construct effectively a code better than a given sequence of codes, in a certain precise sense. As an application, we prove that the existence of a scale of codes (a well-ordered set of codes which contains a code better than any given code) is independent of ZFC.

## 1 Introduction

Lossless coding theory concerns the problem of encoding a sequence of symbols in some alphabet, usually binary. We demand two properties from our codes: they need to be (uniquely) decodable, and they should be concise, that is, the codewords should be short. In this paper we address the following problem: how concise can a coding system for the natural numbers be?

In 1975, Elias [7] considered this problem and constructed a sequence of efficient codes, culminating in the so-called  $\omega$ -code (almost the same code had been discovered by Levenshtein [14] in 1968). The third member in Elias's sequence of codes, called the  $\gamma$ -code, is already asymptotically optimal in the sense that given a non-decreasing high-entropy distribution on the natural numbers, the expected codeword length is almost optimal; consult Elias [7] for a formal definition.

Other concise codes have been constructed by Bentley and Yao [3], Even and Rodeh [8] and Stout [18]. These codes were analyzed by Ahlswede et al. [1]. More recent examples are Yamamoto [22] and Tarau [19]. An online universal code has been constructed by Dodis et al. [5].

A natural question to ask is whether there exists an optimal code. We formulate this question in Section 3 and show that not only is there no single optimal code, but there is also no optimal *sequence* of codes. Since the proofs of these results are constructive, they can be used to construct a fast-growing hierarchy of codes. Elias's construction cannot be used to obtain this result, as we show in Section 3.1.

Care must be taken when considering the *practical* implications of these results: while all codes we consider are effective, they are not necessarily efficient, in the sense that encoding and decoding could be slow. Furthermore, in practice one is not interested in the asymptotic performance of a code, but in its performance on integers up to a certain application-specific bound, or even on a certain class of distributions.

We go on further and consider the existence of a *scale* of codes, which is an uncountable sequence of codes, ordered so that latter codes are better (in the sense of Definition 2.3 below), and containing a code better than any given code. We show in Section 4 that the existence of a scale is independent of ZFC, imitating classical results on functions on the natural numbers ordered by dominance.

## 2 Definitions

We start with some basic notations. The set of all finite binary strings is denoted  $\{0, 1\}^*$ . The set of natural numbers (including zero) is denoted  $\mathbb{N}$ . The set of finite sequences of natural numbers is denoted  $\mathbb{N}^*$ . The length of a binary string  $x$  is denoted  $|x|$ .

Next, some terminology from recursion theory. A sequence  $a(n)$  is called *effective* if the mapping  $n \mapsto a(n)$  is recursive (computable by an algorithm). A sequence  $a_n(m)$  of sequences is effective if the mapping  $(n, m) \mapsto a_n(m)$  is recursive. A real number  $x$  is effective if there is a recursive function mapping  $n$  to a closed rational interval of width at most  $1/n$  containing  $x$  (all rational intervals appearing in this paper are closed).

A sequence  $a(n)$  is effective *relative to* another sequence  $b(n)$  if the mapping  $n \mapsto a(n)$  is recursive given an oracle for the mapping  $n \mapsto b(n)$ . The concept of being effective relative to a sequence of sequences or to a real number is defined analogously. Similarly we can extend the definition to cover sequences of sequences and real numbers which are effective relative to other data.

We proceed to define binary codes, which are our main focus of study.

**Definition 2.1.** A (uniquely-decodable) *binary code* of the natural numbers is a mapping  $C: \mathbb{N} \rightarrow \{0, 1\}^*$  with the property that the function  $C^*: \mathbb{N}^* \rightarrow \{0, 1\}^*$  defined by  $C^*(n_1 \dots n_k) = C(n_1) \dots C(n_k)$  is injective. If furthermore  $|C(n)| \leq |C(m)|$  whenever  $n \leq m$ , then  $C$  is *monotone*.

A *prefix code* has the additional property that  $C(n)$  is not a prefix of  $C(m)$  for any  $n \neq m$ .

Kraft [13] and McMillan [16] proved the following well-known inequality.

**Lemma 2.1** (Kraft's inequality). *Let  $C$  be a binary code. Then*

$$\sum_{n \in \mathbb{N}} 2^{-|C(n)|} \leq 1.$$

*Conversely, given a sequence  $c: \mathbb{N} \rightarrow \mathbb{N}$  satisfying the inequality*

$$\sum_{n \in \mathbb{N}} 2^{-c(n)} \leq 1,$$

*there exists a prefix code  $C$  such that  $|C(n)| = c(n)$ . Furthermore,  $C$  is effective relative to  $c$ .*

Due to this inequality and its converse, our study will concentrate only on the *lengths* of codewords rather than the codewords themselves. This prompts the following definition.

**Definition 2.2.** A *precode* is a monotone non-decreasing function  $c: \mathbb{N} \rightarrow \mathbb{N}$  satisfying Kraft's inequality

$$\sigma(c) \triangleq \sum_{n=0}^{\infty} 2^{-c(n)} \leq 1.$$

A *code* is a precode in which Kraft's inequality is tight. A *proper precode* is a precode in which Kraft's inequality is strict.

The theory can also be developed with respect to non-monotone codes, but we feel that this is less natural. We require that Kraft's inequality be tight for technical reasons (to make our constructions effective). We feel that this is not a large concession since (as we show in Section 3) any binary code can be improved to a binary code in which Kraft's inequality is tight.

Following properties of the sequence of codes constructed by Elias [7], we define a partial order on precodes.

**Definition 2.3.** Let  $c, d$  be precodes. We say that  $c \prec d$  (read  *$c$  is better than  $d$* ) if

$$\lim_{n \rightarrow \infty} c(n) - d(n) = -\infty.$$

We say that  $c \preceq d$  if

$$\sup_{n \rightarrow \infty} c(n) - d(n) < \infty.$$

This definition corresponds to the ratio test for convergent series: indeed, with any precode  $c$  we can associate a convergent series  $c'(n) = 2^{-c(n)}$ , and then  $c \prec d$  if and only if  $c'(n)/d'(n) \rightarrow \infty$ . This differs from the definition used by Cholshechnikova [4] and Vojtáš [21], who apply the ratio test to the remainder term.

Armed with this definition, we can give some evidence to our claim that non-monotone codes are less natural.

**Lemma 2.2.** *There is a function  $d: \mathbb{N} \rightarrow \mathbb{N}$ , satisfying Kraft's inequality tightly, such that  $c \not\prec d$  for any code  $c$ .*

*Proof.* Define  $d$  as follows:

$$d(n) = \begin{cases} k+2 & \text{if } n = 4^k + k - 1, \\ 3k+2 & \text{if } 4^k + k \leq n \leq 4^{k+1} + k - 1. \end{cases}$$

The critical values,  $n = 4^k + k - 1$ , are 0, 4, 17, 66, ... and so on. Let us check that  $d$  satisfies Kraft's equality:

$$\sum_{n=0}^{\infty} 2^{-d(n)} = \sum_{k=0}^{\infty} (2^{-k-2} + 4^k \cdot 2^{-3k-2}) = \sum_{k=0}^{\infty} 2^{-k-1} = 1.$$

If  $c$  is any code then for any  $n$  we have

$$1 > \sum_{m=0}^n 2^{-c(m)} \geq (n+1)2^{-c(n)}.$$

Thus  $c(n) > \log_2(n+1)$ . Choosing  $n = 4^k + k - 1$ , we conclude that

$$c(4^k + k - 1) > \log_2(4^k + k) > 2k.$$

Therefore  $c(4^k + k - 1) \geq 2k + 1 = d(4^k + k - 1) + k - 1$ , and so  $\sup_{n \rightarrow \infty} c(n) - d(n) = \infty$ , that is  $c \not\prec d$ .  $\square$

### 3 Existence of optimal codes

Our goal in this section is to show that there is no optimal code, or even optimal sequence of codes. This is the statement of the following theorem.

**Theorem 3.1.** *For every sequence of codes  $(c_n)_{n \in \mathbb{N}}$  there is a code  $d$ , effective relative to the sequence, such that  $d \prec c_n$  for every  $n \in \mathbb{N}$ .*

Similar results in the related context of fast-growing functions were proved by du Bois-Reymond [6] and Hadamard [10]. Compared to these results, the main challenges in proving Theorem 3.1 are constructing  $d$  in an effective way, and ensuring that  $d$  is monotone.

The first step in proving Theorem 3.1 is constructing effectively a precode  $e$  satisfying  $e \prec c_n$  for every  $n \in \mathbb{N}$ .

**Lemma 3.2.** *For every sequence of codes  $\mathbf{c} = (c_k)_{k \in \mathbb{N}}$  there is a proper precode  $e$ , effective relative to  $\mathbf{c}$ , such that  $e \prec c_k$  for every  $k \in \mathbb{N}$ . Furthermore,  $\sigma(e) \leq 1/2$  and  $\sigma(e)$  is also effective relative to  $\mathbf{c}$ .*

*Proof.* Let  $d(n) = \min_k c_k(n) + k$ . If  $k \geq c_0(n)$  then  $c_k(n) + k > c_0(n) \geq d(n)$ , and so  $d(n) = \min_{k < c_0(n)} c_k(n) + k$ . This shows that  $d$  is effective relative to  $\mathbf{c}$ . Moreover, since the codes  $c_k$  are monotone, so is  $d$ . We will construct a precode  $e \prec d$ , and it will follow (as we show below) that  $e \prec c_k$  for all  $k \in \mathbb{N}$ .

We start by computing a sequence  $(p_m)_{m \in \mathbb{N}}$  satisfying  $\sum_{n=p_m}^{\infty} 2^{-d(n)} \leq 2^{-m}$ . For  $m, k \in \mathbb{N}$  let  $q_{m,k} \geq 1$  be the minimal index satisfying  $\sum_{n=0}^{q_{m,k}-1} 2^{-c_k(n)} \geq 1 - 2^{-m-2}$ , and note that  $\sum_{n=q_{m,k}}^{\infty} 2^{-c_k(n)} \leq 2^{-m-2}$ .

Define  $p_m = \max_{k \leq m+1} q_{m,k}$ . We have

$$\begin{aligned} \sum_{n=p_m}^{\infty} 2^{-d(n)} &< \sum_{n=p_m}^{\infty} \sum_{k=0}^{\infty} 2^{-c_k(n)-k} = \sum_{k=0}^{\infty} 2^{-k} \sum_{n=p_m}^{\infty} 2^{-c_k(n)} \\ &< \sum_{k=m+2}^{\infty} 2^{-k} + \sum_{k=0}^{m+1} 2^{-k} \sum_{n=q_{m,k}}^{\infty} 2^{-c_k(n)} \leq 2^{-m-1} + \sum_{k=0}^{m+1} 2^{-k} 2^{-m-2} < 2^{-m}. \end{aligned}$$

The existence of  $p_0$  implies that  $\sigma(d)$  is convergent, and so  $d(n) \rightarrow \infty$ . Let  $J = \{n \geq 1 : d(n) > d(n-1)\}$ . Since  $d(n) \rightarrow \infty$ ,  $J$  is infinite. The idea now is to construct the sequence  $e$  as follows. Choose an appropriate increasing sequence  $0 = r_0 < r_1 < \dots$ , and let  $e(n) = d(n) - m + C$  for  $r_m \leq n < r_{m+1}$ . We will choose the points  $r_m$  for  $m \geq 1$  from the set  $J$ , and this will ensure that  $e$  is monotone. An appropriate choice of the points  $r_m$  will ensure that  $\sigma(e) < \infty$  is computable (as a function of  $C$ ), and will enable us to choose a value of  $C$  guaranteeing  $\sigma(e) \leq 1/2$ .

The sequence  $(r_m)_{m \in \mathbb{N}}$  is defined as follows. Let  $r_0 = 0$ , and for  $m \geq 1$ , let  $r_m$  be the minimal element of  $J$  which is larger than both  $r_{m-1}$  and  $p_{2m}$ . The sequence  $r$  is clearly effective relative to  $\mathbf{c}$ . Define a sequence  $e'$  by  $e'(n) = d(n) - m$  in the range  $r_m \leq n < r_{m+1}$ . The sequence  $e'$  is also effective relative to  $\mathbf{c}$ . We claim that  $e'$  is monotone. Indeed, if  $r_m \leq n < r_{m+1} - 1$  then  $e'(n+1) = d(n+1) - m \geq d(n) - m = e'(n)$ , and if  $n = r_{m+1} - 1$  then  $e'(n+1) = d(n+1) - m - 1 \geq d(n) - m = e'(n)$  since  $n+1 = r_{m+1} \in J$  implies  $d(n+1) - 1 \geq d(n)$ .

We proceed to show that  $\sigma(e')$  is computable. For all  $m \in \mathbb{N}$  we have

$$\sum_{n=r_m}^{\infty} 2^{-e'(n)} = \sum_{l=m}^{\infty} \sum_{n=r_l}^{r_{l+1}-1} 2^{-d(n)+l} \leq \sum_{l=m}^{\infty} 2^l \sum_{n=p_{2l}}^{\infty} 2^{-d(n)} \leq \sum_{l=m}^{\infty} 2^l 2^{-2l} = 2^{-m+1}.$$

This shows that  $\sigma(e')$  is computable. In particular, we can find an integer  $C$  such that  $\sigma(e') \leq 2^{C-1}$ . Define  $e(n) = e'(n) + C$ . Since  $e'$  is monotone so is  $e$ , and since  $\sigma(e) = 2^{-C} \sigma(e') \leq 1/2$ ,  $e$  is a precode. Moreover,  $\sigma(e)$  is computable.

It remains to show that for all  $k \in \mathbb{N}$ ,  $e < c_k$ . Given  $k, t \in \mathbb{N}$ , for all  $n \geq r_{k+t+C}$  we have

$$e(n) \leq d(n) - k - t \leq c_k(n) - t.$$

This implies that  $e(n) - c_k(n) \rightarrow -\infty$ , and so  $e < c_k$ . □

The second step of the proof of Theorem 3.1 completes the precode constructed in Lemma 3.2 to a code. Given a proper precode  $e$ , we construct a code  $d \preceq e$  by pointwise decreasing  $e$ . The idea is as follows. Suppose that  $2^{-k} \leq 1 - \sigma(e) \leq 2^{-k+2}$ . Find the first  $m$  such that  $e(m) > k$ , and create a new code  $e'$  by setting  $e'(m) = k$  and  $e'(n) = e(n)$  for  $n \neq m$ . The new code satisfies  $\sigma(e') \geq \sigma(e) + 2^{-k-1}$  and so  $1 - \sigma(e') \leq (7/8)(1 - \sigma(e))$ . Repeating this operation, we obtain a code  $d$ .

The main difficulty is computing an integer  $k$  such that  $2^{-k} \leq 1 - \sigma(e) \leq 2^{-k+2}$ . This is accomplished by computing an approximation to  $\log_2(1 - \sigma(e))$ , a function which is the subject of the following routine technical lemma.

**Lemma 3.3.** *Let  $\delta > 0$  be a rational number and let  $x$  be a real number satisfying  $x \leq 1 - \delta$ . Then  $\log_2(1 - x)$  is effective relative to  $x$  and  $\delta$ .*

*Proof.* Let  $\Delta$  be an integer satisfying  $\delta \geq 1/\Delta$ . The function  $f(t) = \log_2(1 - t)$  satisfies  $-C\Delta \leq f'(t) \leq 0$  for  $t \leq 1 - 1/(2\Delta)$ , where  $C = 2 \log_2 e > 1$ . Hence if  $I = [a, b] \subseteq [0, 1 - 1/(2\Delta)]$  is an interval of width  $\ell$  containing  $x$  then  $[f(b), f(a)]$  is an interval of width at most  $C\Delta\ell$  containing  $f(x)$ .

Given non-zero  $n \in \mathbb{N}$ , we show how to compute an interval of length at most  $1/n$  containing  $\log_2(1 - x)$ , given  $\delta$  and an oracle for  $x$ . We start by computing  $\Delta = \lceil 1/\delta \rceil$  and  $N = \lceil 2C\Delta n \rceil \geq 2\Delta$ . We ask the oracle for a rational interval  $[a, b]$  of length at most  $1/N$  containing  $x$ . Since  $1/N \leq 1/(2\Delta)$ , we have

$b \leq x + 1/(2\Delta) \leq (1 - 1/\Delta) + 1/(2\Delta) = 1 - 1/(2\Delta)$ . Therefore  $[f(b), f(a)]$  is an interval of width at most  $C\Delta/N \leq 1/(2n)$  containing  $f(x)$ . Finally, using a Taylor series expansion we compute rationals  $g(a), g(b)$  approximating  $f(a), f(b)$  up to  $1/(4n)$ . The interval  $[g(b), g(a)]$  is a rational interval of width at most  $1/n$  containing  $f(x)$ .  $\square$

Given this technical lemma, we are able to implement the program described above for the second step of the proof of Theorem 3.1.

**Lemma 3.4.** *For any proper precode  $e$  there is a code  $d$ , effective relative to  $e$  and  $\log_2(1 - \sigma(e))$ , such that  $d(n) \leq e(n)$  for all  $n \in \mathbb{N}$ .*

*Proof.* In this proof, whenever we use the term *effective*, we mean effective relative to  $e$  and  $\log_2(1 - \sigma(e))$ .

We construct a sequence  $d_t$  of precodes converging to  $d$  (we make this notion precise below). We will ensure that  $\sigma(d_t) < 1$  and that the sequences  $d_t$  and  $\log_2(1 - \sigma(d_t))$  are effective, and furthermore  $\sigma(d_t)$  is strictly increasing.

The starting point is the sequence  $d_0(n) = e(n)$ . Next suppose that  $d_t$  has been defined. We will find effectively an integer  $k_t$  satisfying

$$2^{-k_t} \leq 1 - \sigma(d_t) \leq 2^{-k_t+2}. \quad (1)$$

Since  $\log_2(1 - \sigma(d_t))$  is effective, we can effectively find an interval  $I_t$  of width at most 1 containing it, and an integer  $k'_t$  such that  $I_t \subset [k'_t - 2, k'_t]$ , implying

$$2^{-k'_t} \leq 1 - \sigma(d_t) \leq 2^{-k'_t+2}.$$

If  $t = 0$  then we put  $k_t = k'_t$ , and otherwise we put  $k_t = \max(k'_t, k_{t-1})$ . If  $k_t = k'_t$  then (1) clearly holds. If  $k_t = k_{t-1}$  then using the assumption  $\sigma(d_t) > \sigma(d_{t-1})$  and the inequality  $1 - \sigma(d_{t-1}) \leq 2^{-k_{t-1}+2}$  we have

$$2^{-k_t} \leq 2^{-k'_t} \leq 1 - \sigma(d_t) < 1 - \sigma(d_{t-1}) \leq 2^{-k_{t-1}+2} = 2^{-k_t+2}.$$

Given  $d_t$  and  $k_t$ , define  $d_{t+1}$  as follows. Let  $m_t$  be the minimal position for which  $d_t(m_t) > k_t$ . The new sequence  $d_{t+1}$  is obtained from  $d_t$  by setting  $d_{t+1}(m_t) = k_t$  and  $d_{t+1}(n) = d_t(n)$  for  $n \neq m_t$ ; our choice of  $m_t$  guarantees that  $d_{t+1}$  is monotone. We have

$$1 - \sigma(d_{t+1}) = 1 - \sigma(d_t) - 2^{-k_t} + 2^{-d_t(m_t)}.$$

Since  $d_t(m_t) \geq k_t + 1$ ,

$$1 - \sigma(d_{t+1}) \leq 1 - \sigma(d_t) - 2^{-k_t-1} \leq \frac{7}{8}(1 - \sigma(d_t)).$$

This shows that  $1 - \sigma(d_t) \rightarrow 0$ . Moreover, it implies that  $k_t \rightarrow \infty$ . Clearly  $\sigma(d_{t+1})$  is effective. Since

$$1 - \sigma(d_{t+1}) \geq 2^{-k_t} - 2^{-k_t} + 2^{-d_t(m_t)} = 2^{-d_t(m_t)},$$

applying Lemma 3.3, we see that  $\log_2(1 - \sigma(d_{t+1}))$  is effective.

We define  $d(n) = \min_t d_t(n)$ . Since  $k_t$  is non-decreasing and  $k_t \rightarrow \infty$ ,  $d$  is effective. Since each  $d_t$  is monotone, so is  $d$ . Clearly  $\sigma(d) \geq \sigma(d_t)$ , hence  $1 - \sigma(d_t) \rightarrow 0$  implies that  $\sigma(d) \geq 1$ . On the other hand, each prefix of  $d$  is a prefix of  $d_t$  for all sufficiently large  $t$ . Since each  $d_t$  is a precode, we deduce that for all  $m \in \mathbb{N}$ ,  $\sum_{n=0}^m 2^{-d(n)} < 1$ , and so  $\sigma(d) \leq 1$ . Put together,  $\sigma(d)$  is a code.  $\square$

We are now ready to prove the main theorem.

*Proof of Theorem 3.1.* Lemma 3.2 shows that there is a proper precode  $e$  satisfying  $e \preceq c_n$  for all  $n \in \mathbb{N}$  which is effective relative to  $\mathbf{c}$ , and furthermore  $\sigma(e) \leq 1/2$  is also effective relative to  $\mathbf{c}$ . Lemma 3.3 implies that  $\log_2(1 - \sigma(e))$  is effective relative to  $\mathbf{c}$ , and so we can apply Lemma 3.4 to obtain a code  $d$  satisfying  $d(m) \leq e(m)$  for all  $m \in \mathbb{N}$  which is effective relative to  $\mathbf{c}$ . This clearly implies that  $d \prec c_n$  for all  $n \in \mathbb{N}$ .  $\square$

### 3.1 Elias's construction

The proof of Theorem 3.1 is somewhat complicated, and one wonders whether there is any simpler construction. In this section we explain Elias's construction, and show that it doesn't always produce a better code.

Elias [7] defines a sequence of codes, starting with the trivial code  $\alpha(n) = n + 1$ . Successive codes in the sequence are defined by applying the following operation.

**Definition 3.1.** Let  $c$  be a code. The *successor code*  $S(c)$  is defined by

$$S(c)(n) = \lfloor \log_2(n+1) \rfloor + c(\lfloor \log_2(n+1) \rfloor).$$

**Lemma 3.5.** For any code  $c$ ,  $S(c)$  is a code which is effective relative to  $c$ .

*Proof.* Clearly  $S(c)$  is monotone and effective relative to  $c$ . It also satisfies Kraft's equality:

$$\sum_{n=0}^{\infty} 2^{-S(c)(n)} = \sum_{m=0}^{\infty} \sum_{n=2^m-1}^{2^{m+1}-2} 2^{-m-c(m)} = \sum_{m=0}^{\infty} 2^{-c(m)} = 1. \quad \square$$

If we start with  $\alpha$  and apply the operation  $S$  successively, then we obtain progressively better codes. However, this phenomenon isn't universal.

**Lemma 3.6.** There exists an effective code  $c$  such that  $S(c) \not\preceq c$ .

*Proof.* The construction proceeds in infinitely many stages. We start with the empty sequence. Suppose that in stage  $n \in \mathbb{N}$ , the sequence is of length  $\ell_n$  (so  $\ell_0 = 0$ ). We add to the sequence  $2^{\ell_n+1}$  copies of the number  $\ell_n + n + 2$ . The resulting sequence has the form  $2, 2, 5, 5, 5, 5, 5, 5, 5, 5, 14, \dots$  and so on.

The sequence is clearly monotone, and the contribution of stage  $n$  to the sum in Kraft's inequality is  $2^{\ell_n+1} \cdot 2^{-\ell_n-n-2} = 2^{-n-1}$ . As  $\sum_{n \geq 0} 2^{-n-1} = 1$ ,  $c$  is a code. To see that  $S(c) \not\preceq c$ , notice that

$$S(c)(2^{\ell_n+1}) = c(\ell_n + 1) + \ell_n + 1 = c(\ell_n + 2^{\ell_n+1}) + \ell_n + 1 \geq c(2^{\ell_n+1}) + \ell_n + 1. \quad \square$$

This lemma shows that Elias's construction cannot be used in place of Lemma 3.2. In the same paper, Elias also defines the  $\omega$ -code, which is obtained through a diagonalization-like construction from the sequence of codes  $S^{(t)}(\alpha)$ . We do not know how to generalize this construction.

## 4 Existence of scale

In the preceding section, we have shown that there is no optimal sequence of codes. However, if we widen our scope by allowing uncountable sequences, such an object could perhaps be found.

**Definition 4.1.** A *scale* of codes  $S$  is a set which is well-ordered with respect to  $\prec$  (every non-empty subset of  $S$  has a maximal element) and is cofinal in the poset of codes (for every code  $c$  there is a code  $d \prec c$  in  $S$ ).

Instead of insisting that the scale be well-ordered, we could instead ask for it to be a chain (any two elements are comparable). Standard arguments show that if such an object exists then so does a scale.

Mimicking a result of Hausdorff [11], we show that a scale exists given that the continuum hypothesis (CH) holds. This follows from Theorem 3.1 using a standard argument.

**Theorem 4.1.** If CH holds then there exists a scale of codes.

*Proof.* We construct a scale  $S = \{s_\alpha : \alpha \in \omega_1\}$  by transfinite induction on  $\omega_1$ , using the fact that the cardinality of the set of codes is  $\mathfrak{c} = \aleph_1$ . Fix an enumeration  $(c_\alpha)_{\alpha < \omega_1}$  of all codes. At step  $\alpha$ , use Theorem 3.1 to construct a code  $s_\alpha \prec \{s_\beta : \beta < \alpha\} \cup \{c_\alpha\}$ , using the fact that  $\alpha$  is countable. By construction,  $S$  is well-ordered. Since  $s_\alpha \prec c_\alpha$  for any code  $c_\alpha$ ,  $S$  is a scale.  $\square$

We can also construct a model in which no scale exists. To that end, following a suggestion by Stefan Geschke [15], we add  $\omega_2$  codes using Cohen's forcing. Theorem 3.1 then implies, using standard arguments, that the poset of codes has no scale. Similar arguments appear in Frankiewicz and Zbierski [9, II.5], Jech [12, §24] and Scheepers [17].

The construction uses the concept of *code prefix*, which represents partial information regarding a code.

**Definition 4.2.** A *code prefix* is a finite non-decreasing sequence  $c(0), \dots, c(n)$  of natural numbers satisfying Kraft's inequality strictly,  $\sigma(c) < 1$ .

We say that a code (or code prefix)  $d$  *extends* a code prefix  $c$  if, as a sequence,  $c$  is a prefix of  $d$ .

The following lemma encapsulates all the information we need to know about codes, gleaned mainly from Theorem 3.1.

**Lemma 4.2.** *Let  $c$  be a code prefix.*

- (a) *The code prefix  $c$  can be extended to a code in infinitely many ways.*
- (b) *Given any code  $d$  and  $n \in \mathbb{N}$ , the code prefix  $c$  can be extended to a code prefix  $b$  such that  $b(m) \leq d(m)$  for some  $m \geq n$ .*

*Proof.* For the first item, let  $c = c(0), \dots, c(n)$  be a code prefix. We can extend  $c$  to a code prefix  $c(0), \dots, c(n+1)$  in infinitely many ways. Any such extension can be extended to a code prefix  $c'$  such that  $\sigma(c') = 1 - 2^{-c(n+1)}$ . Finally, extend  $c'$  to a code by affixing  $c(n+1) + 1, c(n+1) + 2, \dots$  at its end.

For the second item, let  $c = c(0), \dots, c(r)$  be a code prefix, and let  $d$  be a code. Since  $c$  is monotone,  $\sigma(c) = A/2^{c(r)}$  for some integer  $A$ , and so  $\sigma(c) \leq 1 - 2^{-c(r)}$ . Use Theorem 3.1 (with  $c_n = d$  for all  $n \in \mathbb{N}$ ) to construct a code  $e \prec d$ . Find a point  $m \geq \max(n, r+1)$  such that  $e(m) \leq d(m) - c(r)$ . Extend  $c$  by  $e(r+1)+c(r), \dots, e(m)+c(r)$  to form a new sequence  $b$ . Since  $\sigma(c) \leq 1 - 2^{-c(r)}$  and  $2^{-e(r+1)} + \dots + 2^{-e(m)} < 1$ , this results in a code prefix, which satisfies  $b(m) = e(m) + c(r) \leq d(m)$ .  $\square$

We are now in a position to describe the forcing construction. The entire construction takes place inside a countable transitive model  $M$  of ZFC.

**Definition 4.3.** A *code prefix bundle* is an  $\omega_2$ -sequence of code prefixes, only finitely many of which have non-zero length. The forcing  $\mathbb{P}$  consists of the set of code prefix bundles, ordered by  $c < d$  whenever for each  $\alpha < \omega_2$ ,  $c_\alpha$  extends  $d_\alpha$ .

The *support* of a code prefix bundle  $c$ , denoted  $\text{supp } c$ , is the set of  $\alpha < \omega_2$  such that  $c_\alpha$  has non-zero length. The support is always finite.

**Lemma 4.3.** *The forcing  $\mathbb{P}$  satisfies the countable chain condition: every antichain in  $\mathbb{P}$  (a subset  $C \subseteq \mathbb{P}$  in which any two  $c, d \in C$  are incompatible: there is no  $e \in \mathbb{P}$  satisfying  $e < c$  and  $e < d$ ) is at most countable.*

*Proof.* Suppose that  $C$  is an uncountable antichain in  $\mathbb{P}$ . Since the support of any code prefix bundle is finite, the  $\Delta$ -system lemma shows that there is an uncountable subset  $D \subseteq C$  and a finite subset  $S \subseteq \omega_2$  such that  $\text{supp } c \cap \text{supp } d = S$  for all  $c, d \in D$ . For each  $\alpha \in S$  there are only countably many possible code prefixes, and so since  $S$  is finite, there is an uncountable subset  $E \subseteq D$  such that  $c_\alpha = d_\alpha$  for all  $\alpha \in S$  and  $c, d \in E$ . However, since  $\text{supp } c \cap \text{supp } d = S$  and  $c, d$  agree on  $S$  for all  $c, d \in E$ , all code prefix bundles in  $E$  are compatible, contradicting the assumption that  $C$  is an antichain.  $\square$

Let  $G$  be a generic filter over  $\mathbb{P}$ , and construct the model  $M[G]$ , which contains  $G$ . Since  $\mathbb{P}$  satisfies the countable chain condition, the forcing preserves cardinals. In the remainder of the section, we show that  $M[G]$  contains no scale of codes.

We start with some consequences of Lemma 4.2.

**Lemma 4.4.** *Let  $\mathbf{c}$  be the  $\omega_2$ -sequence defined by  $c_\alpha = \bigcup_{f \in G} f_\alpha$ .*

- (a) *For each  $\alpha < \omega_2$ ,  $c_\alpha$  is a code. Moreover, for  $\alpha \neq \beta$ ,  $c_\alpha \neq c_\beta$ .*

(b) Every code in  $M[G]$  has a name in  $M^{\mathbb{P}}$  which depends on countably many coordinates of  $\mathbf{c}$ .

(c) Let  $d \in M^{\mathbb{P}}$  be a name of a code which does not depend on  $c_\alpha$ . Then  $\text{val}(d, G) \not\prec c_\alpha$ .

*Proof.* The first item follows directly from Lemma 4.2(a).

The second item follows from the countable chain condition. Indeed, every code  $c \in M[G]$  (represented as a set of pairs  $(n, c(n))$ ) has a nice name of the form  $\{(n, m), a) : a \in A_{n,m}\}$ , where each  $A_{n,m} \subseteq \mathbb{P}$  is an antichain. Lemma 4.3 shows that each  $A_{n,m}$  is countable, and so  $C = \bigcup_{n,m \in \mathbb{N}} A_{n,m}$  is countable. Each  $a \in C$  has finite support, and so altogether the name depends on countably many coordinates of  $\mathbf{c}$ .

To prove the third item, we show that given  $n \in \mathbb{N}$ , any code prefix bundle  $f$  can be extended to a code prefix bundle  $g$  that forces  $c_\alpha(m) \leq d(m)$  for some  $m \geq n$ . Let  $D = \text{val}(d, G)$ . Using Lemma 4.2(b), we can extend  $f_\alpha$  to  $h_\alpha$  which satisfies  $h_\alpha(m) \leq D(m)$  for some  $m \geq n$ . The value of the prefix  $D(0), \dots, D(m)$  is forced by some code prefix bundle  $k$  extending  $f$ . Since  $d$  doesn't depend on the coordinate  $\alpha$ , we can assume that  $k_\alpha = f_\alpha$ . The code prefix bundle  $g$  extends  $k$  by  $g_\alpha = h_\alpha$ , and by construction it forces  $c_\alpha(m) \leq d(m)$ .  $\square$

Lemma 4.4 allows us to show that the bounding number of the poset of codes is  $\omega_1$  while its dominating number is  $\omega_2$ , implying that there is no scale of codes.

**Theorem 4.5.** *In  $M[G]$  there is no scale of codes.*

*Proof.* Let  $\mathbf{c}$  be the  $\omega_2$ -sequence defined by  $c_\alpha = \bigcup_{f \in G} f_\alpha$ . Suppose  $S$  is a scale of codes. For  $\alpha < \omega_1$ , let  $s_\alpha \in S$  satisfy  $s_\alpha \prec c_\alpha$ . We claim that  $S' = \{s_\alpha : \alpha < \omega_1\}$  is cofinal in the poset of codes. Otherwise, there exists a code  $s \in S$  such that  $s \prec s_\alpha \prec c_\alpha$  for all  $\alpha < \omega_1$ . Yet according to Lemma 4.4(b), such a code has a name which depends only on countably many coordinates of  $\mathbf{c}$ . Considering any other coordinate  $\alpha < \omega_1$ , Lemma 4.4(c) shows that  $s \not\prec c_\alpha$ .

The fact that  $S'$  is cofinal contradicts Lemma 4.4(c) in a different way: according to Lemma 4.4(b), all codes in  $S'$  have names depending (together) on at most  $\omega_1$  coordinates of  $\mathbf{c}$ . Considering any other coordinate  $\alpha < \omega_2$ , Lemma 4.4(c) shows that  $s \not\prec c_\alpha$  for all  $s \in S'$ , contradicting the fact that  $S'$  is cofinal. We conclude that  $S$  cannot have been a scale.  $\square$

## 5 Discussion

**Fast-growing hierarchies.** Theorem 3.1 can be used to construct a fast-growing hierarchy of effective codes. Let  $\mu$  be a countable ordinal, and assign a computable fundamental sequence  $(\alpha^{(i)})_{i \in \mathbb{N}}$  to every limit ordinal  $\alpha < \mu$ . The fast-growing hierarchy  $(c_\alpha)_{\alpha < \mu}$  is defined according to the following rules. The base case is  $c_0(n) = n + 1$ . For a successor ordinal  $\alpha + 1$ , use Theorem 3.1 to construct a code  $c_{\alpha+1} \prec c_\alpha$ . For a limit ordinal  $\alpha$ , use Theorem 3.1 to construct a code  $c_\alpha$  such that  $c_\alpha \prec c_{\alpha^{(i)}}$  for all  $i \in \mathbb{N}$ .

**Cardinal characteristics of the continuum.** Section 4 shows that the existence of a scale of codes is independent of ZFC. However, a more satisfying answer will explain how this phenomenon is related to other cardinal characteristics of the continuum. Specifically, it is known that if we do not require our codes to be monotone, then the resulting poset of codes is Tukey-equivalent to the ideal of measure-zero sets [2, Lemma 4.12]. Todorćević [20] conjectures that our poset is also Tukey-equivalent to the same ideal.

## References

- [1] Rudolf Ahlswede, Te Sun Han, and Kingo Kobayashi. Universal coding of integers and unbounded search trees. *IEEE Trans. Inform. Theory*, 43:669–682, March 1997.
- [2] Tomek Bartoszyński. Invariants of measure and category. In Matthew Foreman and Akihiro Kanamori, editors, *Handbook of Set Theory*, pages 491–555. Springer Netherlands, 2010.



- [3] Jon Louis Bentley and Andrew Chi-Chih Yao. An almost optimal algorithm for unbounded searching. *Inform. Processing Lett.*, 5(3):82–87, 1976.
- [4] N. N. Cholshechnikova. Unsolvability of several questions of convergence of series (in Russian). *Mathematical Notes*, 34(5):711–718, 1983.
- [5] Yevgeniy Dodis, Mihai Pătraşcu, and Mikkel Thorup. Changing base without losing space. In *Proc. 42nd ACM Symposium on Theory of Computing (STOC)*, pages 593–602, 2010.
- [6] Paul du Bois-Reymond. Über asymptotische Werte, infinitäre Approximationen und infinitäre Auflösungen von gleichungen. *Mathematische Annalen*, 8:363–414, 1875.
- [7] Peter Elias. Universal codeword sets and representations of the integers. *IEEE Trans. Information Theory*, 21(2):194–203, March 1975.
- [8] Shimon Even and Michael Rodeh. Economical encoding of commas between strings. *Commun. ACM*, 21(4):315–317, 1978.
- [9] Ryszard Frankiewicz and Pawel Zbierski. *Hausdorff Gaps and Limits*, volume 132 of *Studies in logic and the foundations of mathematics*. Elsevier, 1994.
- [10] Jacques Hadamard. Sur les caractères de convergence des séries à termes positifs et sur les fonctions indéfiniment croissantes (avec note complémentaire). *Acta Mathematica*, 18:319–336, 1894.
- [11] Felix Hausdorff. Untersuchungen über Ordnungstypen IV, V. *Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaftler zu Leipzig, Math.-Phys. Klasse*, 59:84–159, 1907.
- [12] Thomas Jech. *Set Theory*. Springer, third edition, 2006.
- [13] Leon G. Kraft. A device for quantizing, grouping, and coding amplitude modulated pulses. Master’s thesis, Electrical Engineering Department, MIT, 1949.
- [14] Vladimir I. Levenshtein. On the redundancy and delay of separable codes for the natural numbers (in Russian). *Problems of Cybernetics*, 20:173–179, 1968.
- [15] Stefan Geschke (mathoverflow.net/users/7743). When do cofinal chains of universal codings of the integers exist? MathOverflow. URL: <http://mathoverflow.net/questions/32622> (version: 2010-07-20).
- [16] Brockway McMillan. Two inequalities implied by unique decipherability. *IEEE Trans. Information Theory*, 2(4):115–116, 1956.
- [17] Marion Scheepers. Gaps in  $\omega^\omega$ . In Haim Judah, editor, *Set theory of the reals*, volume 6 of *Israel Math. Conf. Proc.*, pages 439–561. Bar-Ilan University, American Math. Society, 1993.
- [18] Q. F. Stout. Improved prefix encodings of the natural numbers. *IEEE Trans. Inform. Theory*, IT-26:607–609, 1980.
- [19] Paul Tarau. Hereditarily finite representations of natural numbers and self-delimiting codes. In *MSFP’10*, pages 11–17. ACM, 2010.
- [20] Stevo Todorčević. Personal communication.
- [21] Peter Vojtáš. Set-theoretic characteristics of summability of sequences and convergence of series. *Comm. Math. Univ. Carolinae*, 28(1):173–183, 1987.
- [22] Hirosuke Yamamoto. A new recursive universal code of the positive integers. *IEEE Trans. Inform. Theory*, 46(2):717–723, March 2000.