SARAJEVO JOURNAL OF MATHEMATICS DOI: 10.5644.SJM.14.1.02
Vol.14 (27), No.1, (2018), 13–24

A GENERALIZATION OF CANTOR'S THEOREM

GIULIO FELLIN

ABSTRACT. One of the most important results in basic set theory is without doubt Cantor's Theorem which states that the power set of any set X is strictly bigger than X itself. Specker once stated, without providing a proof, that a generalization is possible: for any natural exponent m, there is a natural number N for which if X has at least N distinct elements, then the power set of X is strictly bigger than X^m. The aim of this paper is to formalize and prove Specker's claim and to provide a way to compute the values of N for which the theorem holds.

1. CANTOR AND SPECKER

We state Cantor's theorem the following way [1]:

Theorem 1.1. *(Cantor). Let X be a set. There is no injective map $\mathcal{P}(X) \to X$.*

This theorem is related to the Generalized Continuum Hypothesis (GCH):

Hypothesis 1. *Let X and Y be infinite sets. If there are two injective maps $X \to Y$ and $Y \to \mathcal{P}(X)$, then there is a bijection either $X \to Y$ or $Y \to \mathcal{P}(X)$.*

In his 1954 article [10], Ernst Specker proves that GCH implies the Axiom of Choice (AC), in the form that for any nonempty set M there exists a function $f : M \to \bigcup M$ such that $f(x) \in x$. The core of the proof lies in the following result:

Theorem 1.2. *(Specker). Let X be a set. If X has at least five distinct elements, then there is no injective map $\mathcal{P}(X) \to X^2$.*

One should note that Specker's theorem is a "modified version" of Cantor's theorem with X^2 instead of X and a restriction on the number of elements of X. In the same article, Specker claims that this theorem can be generalised from the case of exponent 2 to arbitrary finite exponents m, without providing a proof of his claim[1].

2010 *Mathematics Subject Classification.* 03E99.
Key words and phrases. Power set, Cantor's Theorem.

[1]He says: "Ein entsprechender Satz gilt fr beliebige endliche Exponenten"; we translate this as: "An analogous theorem holds for arbitrary finite exponents".

Our aim is to find a function $F:\mathbb{N}\to\mathbb{N}$ that allows us to state and prove the following:

Theorem 1.3. *(Generalized Cantor). Let X be a set. For any $m\in\mathbb{N}$, if X has at least $F(m)$ distinct elements, then there is no injective map $\mathcal{P}(X)\to X^m$. Moreover, if $F(m)\geqslant 1$ and X has exactly $F(m)-1$ distinct elements, then there is an injective map $\mathcal{P}(X)\to X^m$.*

Notice that by Cantor's and Specker's Theorems we must have $F(1)=0$ and $F(2)=5$.

After this brief introduction and some preliminaries, we will define the function F in section 3 in order to prove the main theorem in section 4. After that, we will provide an algorithm to compute F (section 5) and will conclude giving some numerical data (section 6). Throughout this paper we work in Zermelo-Fraenkel Set Theory[2].

2. Preliminaries

Given two sets X and Y, as usual we write $X\preceq Y$ to claim the existence of an injective map $X\to Y$, and $X\cong Y$ to claim the existence of a bijective map $X\to Y$. It is well-known that $\preceq$ is a non-strict total order, while $\cong$ is an equivalence relation.

Proposition 2.1. *Let X be a well-ordered infinite set, and let $m>0$. Then $X^m\cong X$.*

Proof. We already know this[3] for $m=2$. Suppose that $m=2^n$ for some $n\in\mathbb{N}$ and prove the theorem in this particular case by induction on n.

- $n=0$: $X\cong X^1=X^{2^0}$.
- $n\to n+1$: $X^{2^{n+1}}=\left(X^{2^n}\right)^2\cong X^{2^n}\cong X$.

Trivially, if $m\leqslant m'$ we get $X^m\preceq X^{m'}$. Thus, given m, we can choose $m'>m$ such that $m'=2^n$ for some $n\in\mathbb{N}$. Then $X\preceq X^m\preceq X^{2^n}\cong X$. We deduce our goal from the Cantor-Schröder-Bernstein theorem. □

As usual, denote by V the class of all sets and by $\mathbb{O}n$ the class of ordinals[4]. The function

$$\mathcal{H}:V\to\mathbb{O}n, X\mapsto\{\alpha\in\mathbb{O}n:\alpha\preceq X\}$$

is called *Hartogs function*. The function $\mathcal{H}$ is well-defined, in particular $\mathcal{H}(X)$ is a set whenever X is a set[5].

---

[2] If one assumes the Axiom of Choice, a very simple proof of Theorem 1.3 can be given. If X is infinite, the thesis easily follows by proposition 2.1, Zermelo's well-ordering theorem and Cantor's theorem; while if X is finite the thesis is a direct consequence of lemma 3.3.

[3] Theorem 15.11 in Ageron [1]: Let X be an infinite and well-ordered set. Then $X\cong X+\mathbf{1}\cong 2X\cong X^2$. Tarski further proved [12] that AC is equivalent to a formulation of this theorem without the assumption that X is well-ordered.

[4] For an introduction to ordinals, see for example Ageron [1], lesson 17.

[5] Observations 17.2 in Ageron [1]

Given two sets X and Y, denote by $\operatorname{Inj}(X,Y)$ the set of injective maps $X \to Y$.

3. The minimal values function

For the analytical notions needed in this section, we refer to Davidson & Donsig [3]. Consider the function:

$$f : [e, +\infty[\to \mathbb{R}, x \mapsto \frac{x}{\ln x} \ln 2$$

Clearly, f is continuous. Its derivative is:

$$f'(x) = \frac{\ln x - 1}{(\ln x)^2} \ln 2 > 0 \iff x > e$$

Thus f is increasing within all its domain. Its infimum and its supremum are easily calculated:

$$\inf f = f(e) = e \ln 2$$
$$\sup f = \lim_{x \to +\infty} f(x) = \lim_{x \to +\infty} \frac{x}{\log_2 x} = +\infty$$

Since f is continuous and increasing, it is invertible. Therefore, the following is well-defined:

$$A : [e \ln 2, +\infty[\to [e, +\infty[, x \mapsto f^{-1}(x)$$

Observe that $e \ln 2 \approx 1.88$. Next, the following is well-defined:

$$F : \mathbb{N} \to \mathbb{N}, m \mapsto \begin{cases} 1 + \lfloor A(m) \rfloor & m > 1 \\ 0 & m = 1 \\ 1 & m = 0 \end{cases},$$

where

$$\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{N}, x \mapsto \max\{n \in \mathbb{N} : n \leqslant x\}$$

is the *floor function*, also known as *Gauss' parentheses*.

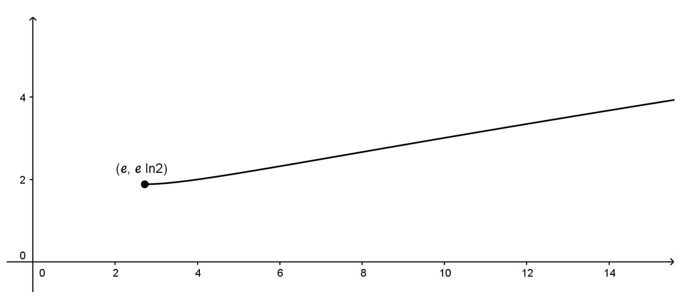

FIGURE 1. Graph of F up to 50.

Similarly, there is the *ceiling function*

$$\lceil\cdot\rceil : \mathbb{R} \to \mathbb{N}, x \mapsto \min\{n \in \mathbb{N} : n \geqslant x\},$$

that will be useful later.

We claim that F is the function we are looking for. To prove so, we need some intermediate results.

Lemma 3.1. *For any $m \in \mathbb{N}_{>1}$ we have that $a = A(m)$ is the minimum value that satisfies*

$$x \in]a, +\infty[\Rightarrow 2^x > x^m.$$

Proof. Fixed $m > 1$, we want to find the minimum value $a \in \mathbb{R}$ that satisfies the desired property. Let's solve the equation $2^x = x^m$. Observe that $A(m)$ is a solution:

$$\begin{aligned} x = A(m) &\Rightarrow m = f(x) \\ &\Rightarrow x^m = \exp(m \ln x) = \exp(f(x) \ln x) = \exp(x \ln 2) = 2^x. \end{aligned}$$

Now we just need to show that $x > A(m)$ implies $2^x > x^m$. Since A is increasing and $e \ln 2 < 2 \leqslant m$ we get that $e = A(e \ln 2) < A(m)$. Moreover, $A(m) \leqslant a$ because $2^{A(m)} \not> (A(m))^m$. We can thus consider $x > A(m)$ and obtain:

$$2^x > x^m \iff m < \frac{x}{\log_2 x} = f(x).$$

Since f is continuous and increasing for $x > e$ and $x = A(m) > e$ is a solution, it follows that

$$\forall x > A(m) : f(x) > f(A(m)) = m,$$

that is equivalent to say that

$$\forall x > A(m) : 2^x > x^m. \qquad \square$$

Lemma 3.2. *Given $m \in \mathbb{N}_{>1}$, the equation $2^x = x^m$ has exactly one solution $B(m)$ in $]1, e[$. Moreover, $B(m)$ satisfies $A(m) - B(m) \geqslant 2$.*

Proof. Consider $x \in]1, e[$. Since $x > 0$ we can write

$$2^x = x^m \iff m = \frac{x}{\ln x} \ln 2.$$

Consider the following function which, apart from its domain, is defined as f:

$$g :]1, e[\to \mathbb{R}, x \mapsto \frac{x}{\ln x} \ln 2.$$

Let's study g analogously as we studied f. Clearly, g is continuous, and its derivative is:

$$g'(x) = \frac{\ln x - 1}{(\ln x)^2} \ln 2 < 0 \iff x < e.$$

Thus g is decreasing within its domain. Its infimum and supremum are:

$$\inf g = \lim_{x\to e} g(x) = \lim_{x\to e} \frac{x}{\log_2 x} = e\ln 2,$$
$$\sup g = \lim_{x\to 1^+} g(x) = \lim_{x\to 1^+} \frac{x}{\log_2 x} = +\infty.$$

Since g is continuous and decreasing, it is invertible. Therefore the following is well-defined:

$$B :]e\ln 2, +\infty[\to]1, e[\,, x \mapsto g^{-1}(x).$$

As before, B is continuous and decreasing. It follows, as for $a = A(m)$, that $B(m)$ is a solution of the starting equation and that it is unique in $]1, e[$. We want an estimate of $A(m) - B(m)$:

$$A(m) - B(m) \geqslant \min_{m\in\mathbb{N}_{>1}} A(m) - \max_{m\in\mathbb{N}_{>1}} B(m) = A(2) - B(2).$$

Let's verify that $4 = A(2)$ and $2 = B(2)$:

$$4 \in]e, +\infty[\,, \qquad 2^4 = 16 = 4^2;$$
$$2 \in]1, e[\,, \qquad 2^2 = 4 = 2^2.$$

In conclusion:

$$A(m) - B(m) \geqslant A(2) - B(2) = 4 - 2 = 2.$$

□

Lemma 3.3. *For any $m > 1$, for any $n \geqslant F(m)$ we have*

$$2^n > n^m,$$

while

$$2^{F(m)-1} \leqslant (F(m) - 1)^m.$$

Proof. Fix $m > 1$. We have:

$$F(m) = 1 + \lfloor A(m) \rfloor > 1 + A(m) - 1 = A(m).$$

Then $F(m) \in]A(m), +\infty[$ and for any $n \geqslant F(m)$ we get $n \in]A(m), +\infty[$. By lemma 3.1 we get $2^n > n^m$. Then, by lemma 3.2

$$B(m) \leqslant A(m) - 2 < A(m) - 1 < F(m) - 1 \leqslant A(m).$$

We have two cases:

(1) $F(m) - 1 \in [e, A(m)]$: for $x \in [e, A(m)]$ (which is in the domain of f) we can write

$$2^x \leqslant x^m \iff m \geqslant f(x).$$

Since f is continuous and increasing for $x > e$ and $x = A(m) > e$ is a solution of $2^x = x^m$, it follows that

$$f(F(m) - 1) \leqslant f(A(m)) = m,$$

i.e.

$$2^{F(m)-1} \leqslant (F(m)-1)^m .$$

(2) $F(m)-1 \in]B(m), e[$: for $x \in]B(m), e[$ we get

$$2^x < x^m \iff m > g(x)$$

(equality is excluded by lemma 3.2). Since g is continuous and decreasing for $x < e$ and $x = B(m) < e$ is a solution of $2^x = x^m$, it follows that

$$g(F(m)-1) < g(B(m)) = m,$$

i.e.

$$2^{F(m)-1} < (F(m)-1)^m . \qquad \square$$

4. A PROOF OF THEOREM 1.3

We first prove separately the case $m = 0$ of theorem 1.3, verifying that $F(0) = 1$. Formally:

Proposition 4.1. *A set X is nonempty if and only if there is no injective map $\mathcal{P}(X) \to \{\emptyset\}$.*

Proof. The direction "$\Leftarrow$" is easily proved by contraposition since $\mathcal{P}(\emptyset) = \{\emptyset\}$. To prove "$\Rightarrow$", observe that there is an injective map $a\colon \{\emptyset\} \to X$. Suppose that there is an injective map $b\colon \mathcal{P}(X) \to \{\emptyset\}$. Then there would be an injection $a \circ b\colon \mathcal{P}(X) \to X$, contradicting Cantor's theorem. $\square$

Lemma 4.2. *Let X be a set, let $m \in \mathbb{N}$ and let $v\colon \mathcal{P}(X) \to X^m$ be an injection. Then for any ordinal $\alpha \geqslant F(m)$, there is a map $u_\alpha : \mathrm{Inj}(\alpha, X) \to X$ such that for any $i \in \mathrm{Inj}(\alpha, X)$ there is $u_\alpha(i) \notin i(\alpha)$.*

Proof. Given m, let α be an ordinal such that $\alpha \geqslant F(m)$. Fix $i \in \mathrm{Inj}(\alpha, X)$ and set $I = i(\alpha)$. Let's build explicitly $u_\alpha(i) \in X \setminus I$ from i.

(1) Suppose that α is finite. Since α is a finite ordinal, we can identify it with a natural number $n \geqslant F(m)$. Then i induces a bijection $\mathbf{n} \to I$; whence I contains exactly n elements and $\mathcal{P}(I)$ contains exactly 2^n elements, as it is well-known. Since v is injective, $v(\mathcal{P}(I))$ has 2^n elements too. By lemma 3.3 we get $|\mathcal{P}(I)| = 2^n > n^m = |I^m|$. It follows that there is $A \in \mathcal{P}(I)$ such that $v(A) \notin I^m$. We can write $v(A) = (x_1, \ldots, x_m)$. Define:

$$u_\alpha(i) := x_k,$$

where $k = \min\{j : x_j \notin I^m\}$.

(2) Suppose that α is infinite. Since α is an infinite ordinal, I is infinite and well-ordered. Then there is a bijection $k : I \to I^m$ (proposition 2.1). Define

$$h : I^m \to \mathcal{P}(I), c \mapsto \begin{cases} v^{-1}(c) & c \in v(\mathcal{P}(I)) \\ \emptyset & \text{otherwise} \end{cases} .$$

Consider $A := \{x \in I : x \notin h \circ k(x)\}$. Suppose that $A = h \circ k(x)$ for some $x \in I$. In this case $x \in A \iff x \notin A$, contradiction. Then $A \notin h \circ k(I) = h(I^m)$. It follows that $v(A) \notin I^m$, since otherwise the definition of h would imply $h(v(A)) = A$. Then we can write $v(A) = (x_1, \ldots, x_m)$ and define

$$u_\alpha(i) := x_k$$

where $k = \min\left\{ j : x_j \notin I^m \right\}$.

We thus defined u_α for any ordinal $\alpha \geqslant F(m)$. □

Proof of theorem 1.3. Case $m = 1$ is Cantor's theorem, while $m = 0$ is proposition 4.1. Let $m > 1$. By lemma 3.3 for any $n \geqslant F(m)$ we have $2^n > n^m$. Suppose that X has at least $F(m)$ distinct elements and that there is an injective map $f : \mathcal{P}(X) \to X^m$. Then there is an injective map $j_{F(m)} : F(m) \to X$. Define by transfinite induction[6] $j_\alpha : \alpha \to X$:

- For $\alpha = F(m)$ we already have $j_{F(m)}$.
- If j_α is defined, define:

$$j_{\alpha+1}(\xi) := \begin{cases} j_\alpha(\xi) & 0 \leqslant \xi < \alpha \\ u_\alpha(j_\alpha) & \xi = \alpha \end{cases},$$

  where u_α is the function defined in lemma 4.2. Since $u_\alpha(j_\alpha) \notin j_\alpha(\alpha)$, we have the injectivity of $j_{\alpha+1}$.
- If λ is a limit ordinal and j_α is defined for every $\alpha < \lambda$, define $j_\lambda(\xi) := j_\alpha(\xi)$ where $\xi < \alpha < \lambda$ (such α exists and j_α does not depend on it). Since all j_α's are injective, j_λ is injective too.

We obtained that every ordinal α is subpotent to X, thus $\mathcal{H}(X) = \mathbb{O}n$ but, since $\mathcal{H}(X)$ is a set, this contradicts the Burali-Forti theorem[7]. For the second statement, observe that if X has exactly $F(m) - 1$ elements then

$$|\mathcal{P}(X)| = 2^{F(m)-1} \leqslant (F(m) - 1)^m = |X^m|.$$

It follows that $\mathcal{P}(X) \preceq X^m$. □

The following result will be useful:

Proposition 4.3. $F(3) = 10$.

Proof. We have:

$$f(9) \approx 2.8392 < 3 < 3.0103 \approx f(10).$$

Since f is increasing,

$$9 < f^{-1}(3) = A(3) < 10.$$

In conclusion, $F(3) = \lfloor A(3) \rfloor + 1 = 10$. □

[6] Principle of transfinite induction, 17.8 in Ageron [1]: Consider a class $H \subseteq \mathbb{O}n$ satisfying: (1) $0 \in H$; (2) $\alpha \in H \Rightarrow \alpha + 1 \in H$; (3) $\lambda = \sup \lambda \wedge (\alpha \in \lambda \Rightarrow \alpha \in H) \Rightarrow \lambda \in H$. Then $H = \mathbb{O}n$.

[7] Theorem 17.5(b) in Ageron [1]: The class $\mathbb{O}n$ is not a set.

5. AN ALGORITHM FOR THE FUNCTION

In this section we want to find an algorithm to compute F. Observe that

$$2^x = x^m \iff x = G(x),$$

where

$$G : \mathbb{R}^+ \to \mathbb{R}^+, x \mapsto m\frac{\ln x}{\ln 2}.$$

Lemma 5.1. *Let $m > 0$. The function $G(x)$ is increasing within its domain. Moreover, for $x > m/\ln 2$ we get $|G'(x)| < 1$.*

Proof. Compute G':

$$G'(x) = \frac{m}{\ln 2}x^{-1}.$$

Clearly, for any x in the domain we have $G'(x) > 0$. Also,

$$x > \frac{m}{\ln 2} \iff \frac{m}{\ln 2}x^{-1} < 1.$$

Then $0 < G'(x) < 1$. In particular, $|G'(x)| < 1$. □

Lemma 5.2. *For any $m \in \mathbb{N}, m \geqslant 2$ we get:*

$$\frac{m}{\ln 2} < 6m - 8.$$

Moreover, if $m \geqslant 4$, then $6m - 8 \leqslant A(m)$.

Proof. For the firs inequality:

$$\frac{m}{\ln 2} < 6m - 8 \iff m > \frac{8\ln 2}{6\ln 2 - 1} \approx 1.76.$$

For the second one, prove the following equivalent property:

$$x \geqslant A(4) \Rightarrow h(x) := 6f(x) - x - 8 \leqslant 0.$$

Compute h':

$$h'(x) = 6f'(x) - 1 = -\frac{(\ln x)^2 - 6\ln 2 \ln x + 6\ln 2}{(\ln x)^2} < 0$$

$$\iff \ln x < 3\ln 2 - \sqrt{3\ln 2(3\ln 2 - 2)} \vee \ln x > 3\ln 2 + \sqrt{3\ln 2(3\ln 2 - 2)}$$

$$\iff 0 < x < e^{3\ln 2 - \sqrt{3\ln 2(3\ln 2-2)}} \approx 5.33 \vee x > e^{3\ln 2 + \sqrt{3\ln 2(3\ln 2 - 2)}} \approx 12.01.$$

In particular, for $x \geqslant A(4) = 16$ we have that h is decreasing. In addition, $h(16) = 6 \cdot 4 - 16 - 8 = 0$, then $x \geqslant 16 \Rightarrow h(x) \leqslant 0$. □

By lemma 5.2, we have that, given $m \geqslant 4$, the fixed-point method applied to G starting in $x_0 = 6m - 8$ converges to the solution of $2^x = x^m$, i.e. to $x^* = A(m)$. In particular, since G is increasing, given $\overline{x} \in [x_0, x^*[$, we have $\overline{x} < G(\overline{x}) < x^*$. We are not interested in the exact value of x^*, but in the one of $F(m) = \lfloor x^* \rfloor + 1$. To this end we could approximate x^* and then compute $F(m)$, but the following lemma will allow us to build a simpler algorithm.

Lemma 5.3. *Let $m > 1$.*

i) *If $A(m) \notin \mathbb{N}$, then $F(m) = \lceil A(m) \rceil$.*
ii) *If $A(m) \in \mathbb{N}$, then $F(m) = \lceil A(m) \rceil + 1$.*

Proof.

i) $\lceil A(m) \rceil = \lfloor A(m) \rfloor + 1 = F(m)$.
ii) $\lceil A(m) \rceil = \lfloor A(m) \rfloor \Rightarrow \lceil A(m) \rceil + 1 = \lfloor A(m) \rfloor + 1 = F(m)$. □

Define

$$\tilde{G} : \mathbb{R}^+ \to \mathbb{N}, x \mapsto \lceil G(x) \rceil$$

Algorithm 1. *Let $m \in \mathbb{N}$ be given in input.*

Case 1: *If $m = 0$, set $N = 1$.*
Case 2: *If $m = 1$, set $N = 0$.*
Case 3: *If $m > 1$:*

(a) *Set $N_0 := 6m - 8$.*
(b) *Recursively, while $N_k < \tilde{G}(N_k)$, set $N_{k+1} := \tilde{G}(N_k)$. Denote by N_n the last element in the sequence.*
(c) *If $N_n = m \log_2 x$, set $N = N_n + 1$, otherwise set $N = N_n$.*

Return N.

Proof. Cases 1 and 2 are Cantor's theorem and proposition 4.1, respectively. If $m \geqslant 4$, by lemma 5.2 we can apply the modified version of the fixed-point method. Cases $m = 2$ and $m = 3$ are easily checked by direct computation (using $F(2) = 5$ and $F(3) = 10$). □

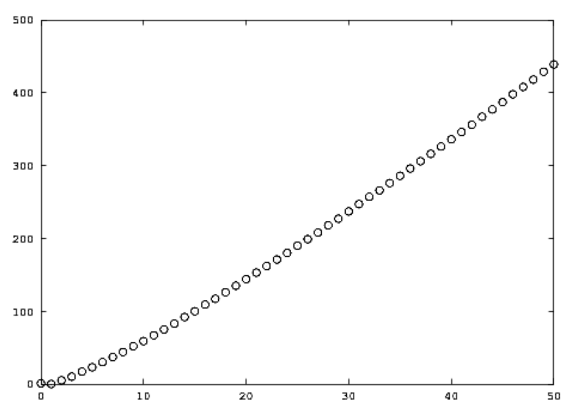

FIGURE 2. Graph of F up to 50.

6. Some numerical data

Let's implement algorithm 1 in Matlab/GNU Octave language[8] and write it in figure 3.

FIGURE 3. Matlab/GNU Octave code for algorithm 1.

```
function N = specker(m)
if m == 0
    N = 1;
elseif m == 1
    N = 0;
else
    g = @(x) ceil(m*log2(x));
    N = 6*m - 8;
    G = g(N);
    while N < G
        N = G;
        G = g(N);
    end
    if N == m*log2(N)
        N = N + 1;
    end
end
end
```

The algorithm 1 is *exact*. We want to observe numerically its complexity, via the number of iterations and time elapsed. Choose a large interval of values of m, for example from 0 to $2^{20} = 1048576$ and compute the minimum, the maximum and the average values of `c` (number of iterations) and of `t` (time elapsed).

```
min(c) = 0           max(c) = 9           sum(c)/m = 7.77033
min(t) = 1.1921e-05  max(t) = 6.4993e-04  sum(t)/m = 2.8193e-04
```

Notice that even for values of m of the order of 10^6 the algorithm terminates in less than ten iterations. Moreover, the elapsed time is also very low, of the order of $10^{-4}s$ ($0.0001s$).

Modify the original code in order to show all the iterations. The trace table can be found in figure 1. Observe the following cases:

(1) For $m \in \{0,1\}$ we immediately get the final result.
(2) For $m \in \{2,4,32,4096\}$ we get $N = N_n + 1$[9].
(3) For all the other values of m we get $N = N_n$.

---

[8]All the codes in this section (and their respective results) were executed by software *Cantor*, an interface for Octave.

[9]It can be shown that m is in this case if and only if $m = 2^{2^k - k}$ for some $k \in \mathbb{N}$.

Notice that, even though the number of iterations has an apparent tendency to increase with m, this isn't a strict rule.

TABLE 1. Trace table for some values of m.

m	N_0	N_1	N_2	N_3	N_4	N_5	N
0	·	·	·	·	·	·	1
1	·	·	·	·	·	·	0
2	4	·	·	·	·	·	5
3	10	·	·	·	·	·	10
4	16	·	·	·	·	·	17
5	22	23	·	·	·	·	23
6	28	29	30	·	·	·	30
7	34	36	37	·	·	·	37
8	40	43	44	·	·	·	44
9	46	50	51	52	·	·	52
10	52	58	59	·	·	·	59
16	88	104	108	109	·	·	109
20	112	137	142	143	144	·	144
32	184	241	254	256	·	·	257
40	232	315	332	336	·	·	336
64	376	548	583	588	589	·	589
100	592	921	985	995	996	997	997
1000	5992	12549	13616	13734	13746	13747	13747
1024	6136	12886	13982	14102	14115	14116	14116
4096	24568	59739	64989	65487	65532	65536	65537

TABLE 2. Some values of F computed by the algorithm.

m	1	2	3	4	5	6	7	8	9	10
N	0	5	10	17	23	30	37	44	52	59
m	11	12	13	14	15	16	17	18	19	20
N	67	75	83	92	100	109	117	126	135	144
m	21	22	23	24	25	26	27	28	29	30
N	153	162	171	180	190	199	208	218	227	237
m	31	32	33	34	35	36	37	38	39	40
N	247	257	266	276	286	296	306	316	326	336
m	41	42	43	44	45	46	47	48	49	50
N	346	356	367	377	387	398	408	418	429	439

REFERENCES

[1] P. Ageron, *Logique, ensembles, catégories. Le point de vue constructif*, Paris, Ellipses Édition, 2000
[2] D.S. Bridges, *The Continuum Hypothesis implies excluded middle*, in “Concepts of Proof in Mathematics, Philosophy, and Computer Science”, edited by D. Probst and P. Schuster, Berlin, Walter de Gruyter, 2016
[3] G. Cantor, *Contributions to the Founding of the Theory of Transfinite Numbers*, New York, Dover Publications, 2010 (reprint of the 1915 edition)
[4] K.R. Davidson and A.P. Donsig, *Real Analysis and Applications. Theory in Practice*, New York, Springer, 2010
[5] A.A. Fraenkel, Y. Bar-Hillel and A. Lévy, *Foundations of Set Theory*, Amsterdam, Elsevier, 1973
[6] P.R. Halmos, *Naive Set Theory*, New York, Van Nostrand Reinhold Company, 1960
[7] S. Leonesi and C. Toffalori, *Matematica, miracoli e paradossi. Storie di cardinali da Cantor a Gödel*, Milan, Bruno Mondadori Editore, 2007
[8] A. Lévy, *Basic Set Theory*, New York, Springer-Verlag, 1979
[9] L. Motto Ros, *Teoria degli Insiemi (prima parte)*, slides from the course “Teoria degli Insiemi” held at the “Scuola Estiva di Logica” in Gargnano, 22-27 August 2016, *https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbn xsdWNhbW90dG9yb3N8Z3g6MTVj*
[10] E.P. Specker, *Selecta*, edited by G. Jäger, H. Läuchli, B. Scarpellini and V. Strassen, Boston, Birkhäuser Verlag, 1990
[11] E.P. Specker, *Verallgemeinerte Kontinuumshypothese und Auswahlaxiom.*, in “Archiv der Mathematik”, August 1954, Volume 5, Issue 4, pp 332-337
[12] A. Tajtelbaum-Tarski, *Sur quelques theorems qui equivalent a l’axiome du choix.*, in “Fundamenta Mathematicae”, 1924, Volume 5, Issue 1, pp 147-154
[13] D. Van Dalen, H.C. Doets and H. De Swart, *Sets: Naive, Axiomatic and Applied. A Basic Compendium with Exercises for Use in Set Theory For Non Logicians, Working and Teaching Mathematicians and Students*, Oxford, Pergamon Press, 1978

(Received: March 21, 2017)
(Revised: July 10, 2018)

Giulio Fellin
University of Verona
Department of Computer Science
Strada le Grazie 15 37134 Verona, IT
giulio.fellin@univr.it