Countability for 1a's

Thomas Forster

May 18, 2016

Contents

None of the stuff that follows below is hard, but it takes a bit of getting used to. And getting used to it is what you're going to have to do, co's it's **basic** and everyone is going to assume you are on top of it. As they used to say in 'Allo 'Allo: "Listen carefully, co's i'm going to say this only *once*".

I am not planning to give rigorous proofs or a huge amount of detail. This is not [part of] a textbook, it's a bundle of notes whose purpose is to give you a feel for which sets are countable and which aren't. However, although it's not part of a textbook, it is pretty comprehensive. If you are on top of everything in the following pages, you will have no worries about countability for a *loooong* time.

1 Preliminaries

I'm assuming that the reader knows what injections, surjections and bijections are, and that they know what it is for a relation to be *transitive* and what an equivalence relation is and what equivalence classes are, so that if $\sim$ is an equivalence relation on a set X then there is a surjection $X \twoheadrightarrow \{[x]_\sim : x \in X\}$, the set of equivalence classes of members of X. (The double barb on the arrow means "surjection"). I am going to assume that the reader is happy with the gadget of *disjoint union*. We will also need the concept of a *congruence relation*. We say $\equiv$ is a congruence relation "for" a function f of n variables if [we illustrate with $n = 2$ to keep things readable]

$$x \equiv x' \ \wedge \ y \equiv y' \quad \to \quad f(x, y) \equiv f(x', y')$$

For example, the equivalence relation on $\mathbb{Z}$ of congruence mod p is a congruence relation for $+$ and $\times$. You almost certainly know this fact already, even if not under that name. Miniexercise: take a moment to check it. Check also that congruence-mod-p is **not** a congruence relation for exponentiation! (you might like to find an illustration of this last fact).

Check that you have these prerequisites under your belt before reading further.

The study of countability is part of cardinal arithmetic, and with cardinal arithmetic the equivalence relation that matters is the equivalence relation on sets of being-in-bijection-with, and it's a congruence relation for all sorts of operations on sets. You can think of cardinals as [arising from] equivalence classes of sets under this equivalence relation. It's sometimes called *equipollence*, and sometimes *equinumerosity*.

We use the double vertical bar notation for cardinals. You will sometimes see the hash symbol used: $\#(x)$, or even (in the older mathematics literature) a double overlining: $\overline{\overline{x}}$. Objects that are $|x|$ for some x are **cardinals**: $|x|$ is **the cardinal number of** the set x.

'$|X| \leq |Y|$' means that there is an injection from X into Y;

'$|X| = |Y|$' means that there is a bijection between X and Y;

'$|X| \leq^* |Y|$' means that there is a surjection from Y onto X.

In most of the cases you will be concerned with (at least for the moment) $|X| \leq^* |Y|$ implies $|X| \leq |Y|$, so you may act on that assumption—at least for the time being. The reader can check that $\leq$ and $\leq^*$ are transitive. We will see later (remark 2 "Cantor-Bernstein") that $\leq$ is antisymmetric.

The equivalence relation of being-in-bijection-with is a congruence relation for disjoint union, cartesian product, and the operation $X \to Y$ that gives you the set of all functions from X to Y. [For your own satisfaction you might wish to check all these allegations[1]].

Thus cardinals support addition, multiplication and exponentiation. Cardinal addition arises from disjoint union, cardinal multiplication from cartesian product. Thus

$$|X| + |Y| = |X \sqcup Y| \text{ and } |X| \cdot |Y| = |X \times Y|$$

...where $x \sqcup y$ is the disjoint union of x and y. Cardinal exponentiation arises from the operation of forming the set of all functions from one set to another. How many functions are there from X to Y? Check that you understand why the answer is $|Y|^{|X|}$. ("Multiply probabilities of independent events"). Check for yourself that $2^{|x|} = |\mathcal{P}(x)|$. ($\mathcal{P}(x)$ is the power set of x, the set of all subsets of x).

If you think about composition of functions you will have no difficulty persuading yourself that the following hold for all cardinals α, β, γ.

Remark 1
(1) $\alpha \leq \beta \to \alpha^\gamma \leq \beta^\gamma$;
(2) $\alpha \leq \beta \to \gamma^\alpha \leq \gamma^\beta$.

The following theorem is very useful. You should know how to state it and how to use it... but you can probably get away with not knowing how to prove it. Mind you, sometimes the proof is lectured in 1a, so you *might* be expected to know it. However knowing how to prove it is not a core skill, and you will almost certainly not have to produce a proof in an exam!

Remark 2 *"Cantor-Bernstein"*

If there is an injection from A into B and an injection from B into A, then there is a bijection between A and B.

Equivalently: the relation $\leq$ on cardinals is antisymmetric.

You will often hear remark 2 referred to as "Schröder-Bernstein".

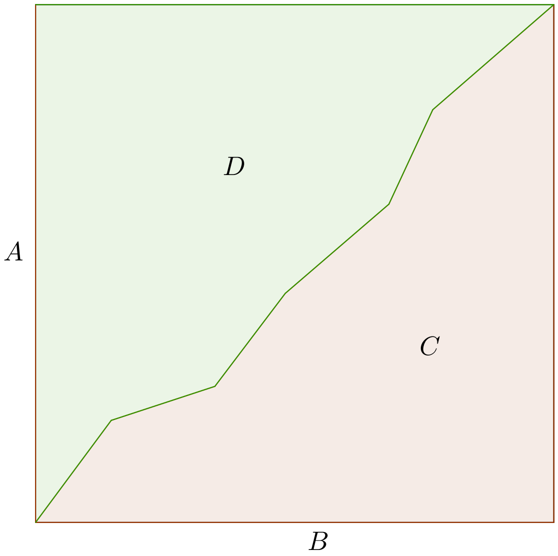
■

You might think this is blindingly obvious: after all, if f injects A into B, and B can be injected into A then f must have been a bijection all along. But this line of talk works only if A and B are finite: if A and B are both infinite you can have injections $f : A \hookrightarrow B$ and $g : N \hookrightarrow A$ neither of which is a surjection. The function that sends the natural number n to the rational number $n/1$ injects $\mathbb{N}$ into $\mathbb{Q}$, and the function that sends the rational number a/b to $2^a \cdot 3^b$ injects the positive rationals into $\mathbb{N}$, but neither f nor g is a surjection.

[1] And do not allow yourself to be confused by the fact that equipollence is a congruence relation for the operation $X \to Y$ that gives you the set of all functions from X to Y even though congruence-mod-p is not a conguence relation for exponentiation: the situations are not parallel.

Remark 3 *Bernstein's lemma*

$$\gamma + \delta = \alpha \cdot \beta \ \to \ \alpha \leq^{*} \gamma \vee \beta \leq \delta$$



Proof: Suppose A and B are two sets (of size α and β). Suppose further that we have split $A \times B$ (represented by the square figure above) into two pieces, C and D (of size γ and δ), so that $C \cap D = \emptyset$ and $C \cup D = A \times B$. Now project the C region onto the A axis. Does it cover the whole of the A-axis? (I've tried to draw the picture so that it's not clear whether it does or not!) If it does, then $|A| \leq^{*} |C|$. If it doesn't, then there is a line through D parallel to the B axis, whence $|B| \leq |D|$.

■

This is quite useful. For example we can use it later to show that if X is a countable set of reals then $|\mathbb{R} \setminus X| = |\mathbb{R}|$.

2 Countable sets

We define $\mathbb{N}$ as the $\subseteq$-least set of cardinals containing 0 and closed under successor:

$$\mathbb{N} = \bigcap\{C : 0 \in C \wedge (\forall x \in C)(x+1 \in C)\}.$$

Definition 1 *We write '$\aleph_0$' for $|\mathbb{N}|$.*

(Don't ask why the funny Hebrew letter and the subscript '0'. There is a reason, but you don't want to hear it just yet.[2] Trust me, i'm a doctor.)

You are a countable set iff you are equipollent with (in 1-1 bijection with) $\mathbb{N}$. Some people still use the word 'countable' in a wider sense that includes finite sets, so don't be surprised if you hear the word used in this way. In that tradition a set is countable iff it is in bijection with *some* set of naturals, not necessarily with the set of *all* naturals. Or, equivalently: X is countable if $|X| = \aleph_0$ or $|X| \in \mathbb{N}$.

Basic useful fact:

Remark 4
$\aleph_0$ is the smallest infinite cardinal: if α is a cardinal with $\alpha \leq \aleph_0$ then $\alpha \in \mathbb{N} \vee \alpha = \aleph_0$. Equivalently: $\alpha \in \mathbb{N} \longleftrightarrow \alpha < \aleph_0$.

Proof: This is because if you are a set of size $\leq \aleph_0$ then there is an injection from you into $\mathbb{N}$, so you are the same size as a set of natural numbers. Now every set of natural numbers is either bounded (in which case it is of size n for some $n \in \mathbb{N}$) or unbounded. If it is unbounded then it is clearly in bijection with $\mathbb{N}$—count it, using the order structure it has in virtue of being a subset of $\mathbb{N}$! ■

In fact $\aleph_0$ is minimal among infinite cardinals even w.r.t. the weaker relation $\leq^*$: we can show that a surjective image of a countable set is countable. If you are the surjective image of a countable set then without loss of generality you are a surjective image of $\mathbb{N}$. But then it's easy to put you in 1-1 correspondence with a set of natural numbers: pair off each of your members with the first element of the preimage.

(To be formal about it, if $f : \mathbb{N} \twoheadrightarrow X$ you inject $X \hookrightarrow \mathbb{N}$ by sending each $x \in X$ to the least natural number in f^{-1}"$\{x\}$. 'f^{-1}"$\{x\}$' (also written '$f^{-1}(\{x\})$') is $\{n \in \mathbb{N} : f(n) = x\}$, commonly described as a **fibre** of f . . . you might find this terminology useful.)

This minimality of $\aleph_0$ is important, and it can save you a lot of time. It means that if you want to show that a set is countable you don't have to go the extreme lengths of finding a bijection between it and the whole of $\mathbb{N}$: it suffices to find a bijection between it and an infinite subset of $\mathbb{N}$.

Another manifestation of this minimality is the following fact:

[2] Yes, there is a cardinal $\aleph_1$ but . . . !!

Remark 5 *For α a cardinal, $\alpha = \alpha + 1 \longleftrightarrow \alpha \geq \aleph_0$.*

Some people take "$\alpha = \alpha + 1$" to be the *definition* of α being an infinite cardinal. The usual definition is $\alpha \not< \aleph_0$ or—equivalently—$\alpha \notin \mathbb{N}$.

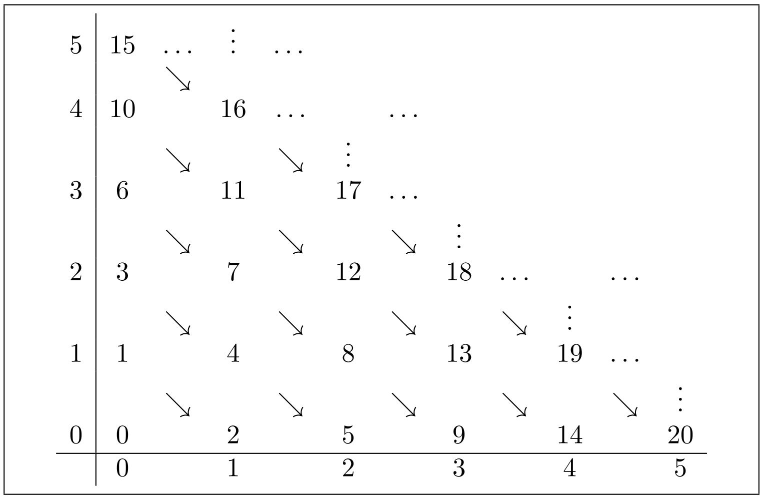
You might like to prove remark 5 for yourself. Catchphrase: *Hilbert's Hotel*... you might like to google it.

Let's now have some examples of sets that are countable

$\aleph_0 + 1 = \aleph_0$; Add an extra member to a countable set: the result is countable.

$\mathbb{N} \sqcup \mathbb{N}$ is countable, which is to say $\aleph_0 + \aleph_0 = \aleph_0$. So $\mathbb{Z}$ is countable, co's it's the union of two copies of $\mathbb{N}$: $\mathbb{N}$ itself and the negative integers.

$\mathbb{N} \times \mathbb{N}$ is countable by **zigzagging**, so we can conclude that $\aleph_0 \cdot \aleph_0 = \aleph_0$.



The fact that the cartesian product of two countable sets is countable can be very useful. If each A_i with $i \in \mathbb{N}$ is a countable set equipped with a counting then you can use those countings to do the same zigzag construction that counts $\mathbb{N} \times \mathbb{N}$ to count the union $\bigcup_{i \in \mathbb{N}} A_i$. The zigzag algorithm needs those countings to work on, of course, so to say—as people often do—that this shows that *a union of countably many countable sets is countable* is not straightforwardly correct. You need an axiom that says that

$$(\forall x)(\exists y)F(x, y) \ \rightarrow \ (\exists f)(\forall x)F(x, f(x))$$

which will reassure you that if all your A_i have countings then there is a function that, to each A_i, assigns a counting of it; you then use those assigned countings in your run of the zigzag algorithm. This axiom is called the "Axiom of Choice" and you will be hearing more of it later.

The following observation will turn out to be very useful:

Remark 6 *(The* **Prime Powers Trick***)*
The set of finite sequences from a countable set form a countable set.

Proof: We map finite sequences of naturals to naturals by sending—for example—the tuple $\langle 1, 0, 8, 7, 3\rangle$ to $2^{1+1} \cdot 3^{0+1} \cdot 5^{8+1} \cdot 7^{7+1} \cdot 11^{3+1}$. ■

Then the set of finite subsets of a countable set is countable because it is a surjective image of the set of finite sequences from that set—and we saw above that a surjective image of a countable set is countable.

We can show $|\mathbb{Q}| = \aleph_0$ by injecting $\mathbb{N}$ into $\mathbb{Q}$ (send the natural number n to the rational number n) and injecting $\mathbb{Q}$ into $\mathbb{N} \times \mathbb{N}$ (send x/y—with no common factors—to $\langle x, y\rangle$) and then using remark 2.

We can think of $\mathbb{Q}$ as a quotient of $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. Say $\langle x, y\rangle \sim \langle u, v\rangle$ iff $x \cdot v = y \cdot u$. Then we can think of the equivalence classes as rationals. If we think of $\mathbb{Q}$ that way then it is clear that it is countable because it's an infinite surjective image of a countable set.

3 Uncountable sets

Are there any? Yes–there are, but it's a nontrivial fact that not all infinite sets are countable. The key fact here is **Cantor's theorem** which tells us that every set is smaller than its power set. Or—to put it another way—$\alpha < 2^\alpha$ for all cardinals α. What we actually prove is—on the face of it—slightly stronger.

Theorem 1 *Cantor's theorem.*

$$|\mathcal{P}(X)| \not\leq^* |X|$$

Proof:

Suppose $f : X \to \mathcal{P}(X)$. We will prove that f is not surjective. Suppose *per impossibile* that it were. Consider $r = \{x \in X : x \notin f(x)\}$. We will show that r cannot be in the range of f. For suppose r were $f(a)$. We consider the proposition

$$¿a \in r?$$

By definition of r this is equivalent to

$$a \in f(a)$$

but $f(a) = \{x \in X : x \notin f(x)\}$ so this is equivalent to

$$a \notin f(a)$$

but $f(a) = r$ so this is equivalent to

$$a \notin r$$

So we have proved $a \in r \longleftrightarrow a \notin r$ which is self-contradictory. ■

Notice that we have proved $a \in r \longleftrightarrow a \notin r$ (which is not explicitly a contradiction) rather than $a \in r \wedge a \notin r$ (which is). It's possible to derive the conjunction from the biconditional but it's a bit fiddly and unless you are a compsci student of a particularly theoretical cast of mind you may well feel that you can put off the task of mastering the fiddly bits until later. However it is worth understanding this proof… at some point—even if not this very minute and second—since echoes of it reappear in the proof of the unsolvability of the Halting Problem for Turing machines, and the derivation of Russell's paradox, among others.

In particular there is no surjection $\mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$.

Observe that we have made no assumptions about the size of X whatever! We haven't even assumed that X is nonempty, and certainly not that it is finite. Do not waste time trying to prove Cantor's theorem for natural numbers by mathematical induction! (And **do not** try to connect this with any ideas you might have about complex exponentiation: different beast altogether!!)

While we are about it we may as well make a note of the fact that the power set of $\mathbb{N}$ is the same size as the reals:

Theorem 2 $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$

It's perhaps not *blindingly* obvious that there is a bijection between $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$. The obvious thing to try—think of a real as a binary expansion, and send it to the set of addresses at which it has a '1'—doesn't quite work, because of double counting of dyadic rationals (rationals with denominator a power of 2) but there are various ways round the problem. One rather neat one (due to my supervisee Jonathan Holmes) is to reflect that every real number has at most one binary representation that contains infinitely many 0s. The set of these representations is in bijection with $\mathcal{P}(\mathbb{N})$! You can also use Bernstein's lemma, remark 3.

I like to think that the difficulty in finding this bijection reflects the fact that $\mathbb{R}$ is a continuous ("analogue") object while $\mathcal{P}(\mathbb{N})$ is a discrete ("digital") one, but I don't want to make *toooo* much of it!

> You should not expect[a], for the moment at least, to encounter any infinite sets of sizes other than $\aleph_0$ and $2^{\aleph_0}$. In particular, any uncountable set you encounter is almost guaranteed to be of size at least $2^{\aleph_0}$.
>
> [a] Of course if you are a Part II student looking at this for revision this warning does not apply to you!

There are uncountable sets that might not be as big as the reals but you do not need to know about them for the moment.

4 Recognising the difference

It's very important to get a feel for which sets are countable and which are uncountable, and to be able to spot which is which without having to go through a laborious proof or computation. On the face of it, if one is to prove that a set is countable one has to show how to count it, and if one is to show that it is uncountable one has to use a diagonal argument as in the proof of Cantor's theorem, remark 1. However there are some heuristics one can use, and I am going to tell you about one that my students have found helpful.

When confronted with a set (as it might be, one of the suspects from the exercise below) one of the things can one do to ascertain whether it is countable or not is to ask "How much information do I have to give to specify a member of this set X?" If the answer is "a finite amount" then X is countable. This is because if we have a way of specifying every member of X then we have a surjection onto X from the set of strings over some finite alphabet and we know that the set of such strings is countable because of the prime powers trick, remark 6. If the answer is "an infinite amount" then the set before you is most assuredly uncountable, and of size at least $2^{\aleph_0}$ at that.

If you have any intuition around expressions like "finite precision", "infinite precision" then you can put it to good use here. Reals are infinite precision objects: to specify a real you need to supply a digit between 0 and 9 for each of **infinitely many** decimal places—independently! The expression 'degree of freedom' might have some resonance for you. . . a point in the plane has two degrees of freedom ("coordinates"); a circle in the plane has three degrees of freedom: two to locate the centre and a third to tell you the radius. (That's why you can draw a circle through any three points. An ellipse has an extra degree of freedom—the eccentricity—so you can draw an ellipse through any four points—OK, as long as no three of them are collinear!) The number of objects you get is the number of options at each parameter raised to the power of the number of degrees of freedom (= the number of parameters).

In this sense, a real number has infinitely many degrees of freedom or—as you will later learn to say—a real number has *infinite entropy*. This is enough to show that there are uncountably many reals. You don't really need to know why this is the case, since what I am offering you here is a *heuristic* not a theorem.

In this hand-wavy sense, one can say that the natural numbers have finite entropy. How so? How many bits of information do I need to have available if I want to transmit a natural number to you? Now you have probably learnt in Probability 1a that there is no probability distribution on the natural numbers that makes them equally probable. So suppose I pick natural number n with probability 2^{-n}. How many bits do I need *on average* to communicate a natural number to you? Well, half the time the number is 1, so I need only one bit, one quarter of the time it'll be 2, so i'll need two bits. It's easy to see (sum the geometric progression) that on average I will need only two bits. So the natural numbers (with this distribution) have an entropy of two bits. With a different distribution you'll get a different entropy, but you are not to worry about that [no, really!![3]]; the point is that there is a way a finding a probability distribution for $\mathbb{N}$ that gives the naturals finite entropy, whereas there is no way of doing that for the reals. Moral: the naturals (unlike the reals) are a countable set.

Don't worry if this looks hand-wavy—it is; it's a heuristic not a theorem. If it works for you that's cool, and if it doesn't, don't worry—forget the previous paragraph entirely. [snaps fingers: wake up now!].

So how many reals are there, if you think of them in binary? You have $\aleph_0$ independent trials (one at each binary place) and each trial has 2 possible outcomes. So the number of reals must be $2^{\aleph_0}$. (if I think of them in decimal I get $10^{\aleph_0}$ and you can show that to be the same). Try another example: how many sets $X \subseteq \mathbb{N}$ of prime powers are there that, for every prime p, contains precisely one power of p? Clearly I can choose my powers of p independently, so there are precisely $\aleph_0^{\aleph_0}$ such sets. Now observe, using remarks 2 and 1

$$2^{\aleph_0} \;\leq^{(a)}\; \aleph_0^{\aleph_0} \;\leq^{(b)}\; (2^{\aleph_0})^{\aleph_0} \;=\; 2^{(\aleph_0{}^2)} \;=^{(c)}\; 2^{\aleph_0}$$

(a) and (b) both hold by remark 1 part (1);
(c) holds because $\aleph_0^2 = \aleph_0$.

Finally we infer

$$2^{\aleph_0} = \aleph_0^{\aleph_0}$$

from

$$2^{\aleph_0} \leq \aleph_0^{\aleph_0} \text{ and } \aleph_0^{\aleph_0} \leq 2^{\aleph_0}$$

by using remark 2.

5 Exercises

(1) (i) Check that $\aleph_0 + 2^{\aleph_0} = 2^{\aleph_0}$.
(ii) Check that $\aleph_0 + \alpha = 2^{\aleph_0} \to \alpha = 2^{\aleph_0}$. (Use Bernstein's Lemma).

(2) Which of the following sets are countable and which are uncountable?

(i) The set of complex numbers;
(ii) The set of partitions of $\mathbb{N}$ into finite pieces;
(iii) The set of partitions of $\mathbb{N}$ into finitely many pieces;
(iv) The set $\mathbb{Q} \to \mathbb{R}$ of functions from the rationals to the reals;
(v) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = 0$ for all but finitely many n;
(vi) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = 0$ or 1 for all but finitely many n;
(vii) The set of functions $f : \mathbb{N} \to \mathbb{N}$ s.t $f(n) = n$ for all but finitely many n;
(viii) The set of ("nonincreasing") functions $f : \mathbb{N} \to \mathbb{N}$ s.t $(\forall n)(f(n) \leq n)$;
(ix) The set of subsets of $\mathbb{N}$ with finite complement ("cofinite");

[3] If you really want to think about this, perhaps have a look at the appendix.

(x) The set of algebraic numbers;
(xi) The set of nonincreasing *partial* functions $\mathbb{N} \to \mathbb{N}$.

Of the sets that are uncountable say—with reasons—whether they are of size $2^{\aleph_0}$ or of size $2^{2^{\aleph_0}}$. You need not give a rigorous proof.

(3) How many injective functions $f : \mathbb{R} \hookrightarrow \mathbb{R}$ are there which satisfy $(\forall xy)(x \leq y \to f(x) \leq f(y))$? Are there $2^{\aleph_0}$ or $2^{2^{\aleph_0}}$?

(4) (2014.4.II.7E, modified) How many ω-sequences are there from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ that agree at infinitely many places with the decimal expansion of $\sqrt{2}$?

(5) Say two permutations of $\mathbb{N}$ are *equivalent* if they agree at all but finitely many arguments. What can you say about how many equivalence classes there are?

(6) If you have done some number theory (so you can remember what a multiplicative function is!) and are doing this for revision...
How many multiplicative functions $\mathbb{N} \to \mathbb{N}$ are there?
How many multiplicative functions $\mathbb{N} \to \mathbb{C}$?

6 Appendix

[with thanks to Ted Harding]

Here's a strategy for identifying a natural number uniquely using only finitely many bits. You ask "Is it greater than 1?", "Is it greater than 2?", "Is it greater than 4?", "Is it greater than 2^n?"... until you get the answer "no!", at $n = k$, say. Then you have located it in the block $[2^{k-1}, 2^k]$, whereupon you start asking "Is it between 2^{k-1} and $2^{k-1} + 2$?"; "Is it between 2^{k-1} and $2^{k-1} + 4$?" ...so you will locate m in no more than $\binom{m}{2}$ steps. There is no global finite bound (independent of m) on the number of questions you might have to ask, but you only ever have to ask finitely many.

But one can always find k with k questions: "Is it 1?"; "is it 2?", "is it 3?"...

This isn't really the same situation as the reals, co's these binary choices are not independent.

7 Afterthoughts

By thinking about degrees of freedom one persuades oneself that the answer to (5) should be "at least $2^{\aleph_0}$", and there is an easy proof that it is, indeed, at least $2^{\aleph_0}$, but the proof can be tricky to find. Here is a cute answer that occurred to me on my bike. [Well, actually, the *question* occurred to me on my bike.] Fix a conditionally convergent series, such as the Alternating Harmonic series, whose general term is $n^{(-1)^n}$. We know that by judiciously ordering the naturals we can get it to sum to any real that we like. (Alice biting from the two sides of the mushroom to get her to the correct height). This gives us an injection

$i : \mathbb{R} \hookrightarrow$ the set of all permutations of $\mathbb{N}$. Now reflect that two permutations of $\mathbb{N}$ that differ on only finitely many arguments will give arrangements that sum to the same real. This means that all the permutations that are the values of this injection i belong to different equivalence classes. This gives us our lower bound of $2^{\aleph_0}$.