Problem Set Week 11 Solutions

Math Olympiad Club Zurich

Spring 2025

Problem 1 (Bernoulli Competition 20203)

1. Let $A = \{1, 2, \dots, 100\}$ be the set of integers between 1 and 100.

(a) Let $B \subset A$ be a subset that doesn't contain two consecutive integers. What is the maximal cardinality of B?

(b) Let $C \subset A$ be a subset such that there is no n for which n and $2n$ are both in C. What is the maximal cardinality of C?

Solutions:

(a) One can easily construct a legal set B with 50 elements by setting it equal to the set of odd numbers from 1 to 100, or the set of even numbers from 1 to 100. That leaves proving that one cannot do better. In order to do that, observe that A can be partitioned into 50 pairs of an odd number and the next even number, i.e. $A = \{1, 2\} \cup \{3, 4\} \cup \dots \cup \{99, 100\}$. B can contain at most one element of each of these pairs, so it has at most 50 elements. Therefore, the maximum possible cardinality of B is 50.

Alternate solution One can easily construct a legal set B with 50 elements by setting it equal to the set of odd numbers from 1 to 100, or the set of even numbers from 1 to 100. That leaves proving that one cannot do better. In order to do that, first let $x_1, \dots, x_m$ be the elements of B in increasing order. The fact that no two elements of B are consecutive implies that $x_{i+1} \geq x_i + 2$ for all i, so $x_m \geq x_1 + 2(m-1) \geq 2m - 1$. However, $x_m \leq 100$ due to being in A, so it must be the case that $m \leq 50$. Therefore, the maximum possible cardinality of B is 50.

(b) For each nonnegative integer m, let $A_m = A \cap \{(2m+1)2^i : i \in \mathbb{Z}\}$, and observe that these are disjoint and $A = \cup_{0 \leq i \leq 49} A_i$. The requirement on C is equivalent to saying that it never contains both $(2m+1)2^i$ and $(2m+1)2^{i+1}$, so $|C \cap A_i| \leq \lfloor |A_i|/2 \rfloor$ by an argument from the solution to the previous part. We can ensure that $|C \cap A_i| = \lfloor |A_i|/2 \rfloor$ for all m, such as by having C be the set of every element of A that can be expressed as an odd number times a power of 4. There are 50 odd numbers in A, 13 odd multiples of 4, 3 odd multiples of 16, and 1 odd multiple of 64. So, C has a cardinality of $50 + 13 + 3 + 1 = \boxed{67}$.

Alternate solution: Observe that for any $51 \leq m \leq 100$, if we let $C' = C \cup \{m\} \backslash \{m/2\}$ then C' contains at least as many elements as C and does not contain both n and $2n$ for any n. So, we can assume that C contains n for all $51 \leq n \leq 100$. In this case, it cannot contain any $26 \leq n \leq 50$. Then by the same logic we can assume that C contains $\{13, \dots, 25\}$, which forces it not to contain any $7 \leq n \leq 12$. Then we can assume that it contains $\{4, 5, 6\}$, which means it does not contain 2 or 3, at which point we can have it contain 1. So, the maximum possible cardinality of C is $50 + 13 + 3 + 1 = \boxed{67}$.

Problem (selected real analysis problem)

Determine whether there exists a continuous function $f : \mathbb{R} \to \mathbb{R}$ (standard topology) such that $f \circ f = F$ where $F(x) = -x$, $F(x) = \exp(x)$, $F(x) = x^2 - 2$,

Solution:

(a) No, first f must be bijective. Prove that $f(0) = 0$ and investigate the sign of $f(x)$ for $x > 0$.

(b) Prove that f is strictly increasing and that $\inf f = a \in (-\infty, 0)$, $f(a) = 0$. Fix an arbitrary strictly increasing function $f_0 \in C([a, 0])$ satisfying the conditions $f_0(a) = 0$ and $f_0(0) = e^a$, and extend it to $\mathbb{R}$ by using the equation.

(c) Prove that f must be strictly increasing on $[0, +\infty)$ and strictly decreasing on $(-\infty, 0]$ and that $f(0) \geq 0$, which is impossible, because F, and hence f, takes negative values.

Bonus: If $F(x) = \cos(x)$?

Solution:

To begin we do some preliminary work (some of the result are well known but for the sake of completeness we give the "proofs"):

-The function cos has a unique fixed point over $\mathbb{R}$ ($\exists! \alpha \in \mathbb{R}\, (cos(\alpha) = \alpha)$) which is moreover located between $]0, 1[$. We define in a classical manner (for this kind of fixed point problem) the function:

$$\varphi : \quad \mathbb{R} \longrightarrow \mathbb{R}$$

$$x \longmapsto x - cos(x) = x - \textstyle\sum_{i \in \mathbb{N}} (-1)^i \cdot \frac{x^{2 \cdot i}}{(2 \cdot i)!}$$

φ is clearly $C^\infty(\mathbb{R})$ and even analytic. We study φ and show that in fact it has only one zero: $|\varphi^{-1}[\{0\}]| = 1$ which will conclude the existence and unicity of the fixed point over $\mathbb{R}$. Notice that $\frac{d}{dx}(\varphi) = 1 - sin \geq \underline{0}$. The theorem relating the type of monotonicity and the sign of the derivative tell us therefore that φ is increasing. As $\varphi(0) = -1$ and $\varphi(1) = 1 - cos(1) \overset{1 \in]0; \frac{\pi}{2}[}{>} 0$, we have that:

$$\varphi[]-\infty; 0]] \subset]-\infty; -1] \subset]-\infty; 0[$$

and

$$\varphi[[1; +\infty[] \subset [\varphi(1); +\infty[\subset]0; +\infty[$$

Thus $\varphi^{-1}[\{0\}] \subset]0; 1[$ and moreover we have by the intermediate value theorem (or the more general topological version: image of a connected set through a continuous function is connected and knowing that only the intervals are precisely the connected set of $(\mathbb{R}, \mathcal{T}_{\mathbb{R}})$) that $0 \in [-1; \varphi(1)] \subset \varphi[[0; 1]]$. This shows that $|\varphi^{-1}[\{0\}]| \geq 1$. We know by the property of sin:

$$\forall x \in \mathbb{R}((\frac{d}{dx}(\varphi))(x) = 0 \leftrightarrow x \in \frac{\pi}{2} + 2 \cdot \pi\mathbb{Z})$$

Therefore we have the refinement that φ is strictly increasing over each connected component of $\mathbb{R} \setminus (\frac{\pi}{2} + 2 \cdot \pi\mathbb{Z})$. However $]\frac{\pi}{2} - 2 \cdot \pi; \frac{\pi}{2}[$ is one of the connected component. This means that φ is strictly increasing over $]0;1[\subset]\frac{\pi}{2}-2\cdot\pi;\frac{\pi}{2}[$ in particular it is injective. We saw that $\varphi^{-1}[\{0\}]\subset]0;1[$ so this means that $|\varphi^{-1}[\{0\}]|=1$. This concludes that there is a unique fixed point of *cos* over $\mathbb{R}$. For the culture, this fixed point is called the *Dottie* number. The decimal expansion of the Dottie number is 0.739085133215160641655312087673873404... and one can show using some advanced techniques like the Lindemann–Weierstrass theorem that it is also a transcendental number. How can we attain such a number ? It is easy: *cos* is a contraction on $[0;1]$! Indeed its derivative $(-sin)$ is continuous therefore bounded over the compact $[0;1]$ and it appears that those bound are strictly less than 1 ! To be more precise, let $a,b\in[0;1]$, when $a\neq b$ we have by the mean value theorem ($cos\in C^{\infty}(\mathbb{R})$) that $\exists c\in]a;b[$ such that $-sin(c)=(\frac{d}{dx}cos)(c)=\frac{cos(a)-cos(b)}{a-b}$. Therefore we obtain:

$$|cos(a)-cos(b)|\leq max|-sin|[[0;1]]\cdot|a-b|$$

$$\overset{sin\text{ is strictly increasing over }[0;\frac{\pi}{2}]}{=} sin(1)\cdot|a-b|$$

This bounds (which works even for $a=b$) shows that *cos* is a contraction over $[0;1]$ **provided** $sin(1)<1$ which is the case since *sin* is strictly increasing over $[0;\frac{\pi}{2}]$ ($1<\frac{\pi}{2}$ so that $sin(1)<sin(\frac{\pi}{2})=1$). Therefore a common application of the Banach fixed point theorem for the complete metrix space $([0;1],|\cdot|)$ tell us not only that there is a unique fixed point of *cos* over $[0;1]$ (we already know this information) but also the way the fixed point is constructed. Take any $x\in[0;1]$, the fixed point is the limit ($[0;1]$ is complete) of the sequence $(cos^{\circ n}(x))_{n\in\mathbb{N}}\in[0;1]^{\mathbb{N}}$ where $cos^{\circ n}$ denotes the functional composition of *cos* with itself n times ($cos^{\circ 0}=Id$). This means that $lim_{n\to+\infty}(cos|_{[0;1]})^{\circ n}=cte_{\alpha}$ where α is the Dottie number. Apparently the generalized case $cos(z)=z$ where $z\in\mathbb{C}$ has infinitely many solutions (it uses Picard's theorem).

-Let us denote the Dottie number by $\alpha\in]0;1[$. We claim that any function $g:\mathbb{R}\to\mathbb{R}$ satisfying $g\circ g=cos$ share the same fixed point of *cos* namely α and must be injective over $[0;\frac{\pi}{2}]$. Indeed suppose $g\circ g=cos$ then:

$$cos(g(\alpha))=(g\circ g)(g(\alpha))=g((g\circ g)(\alpha))=g(cos(\alpha))=g(\alpha)$$

Therefore $g(\alpha)$ is a fixed point of *cos*, by the unicity of the Dottie number we must have $g(\alpha)=\alpha$. The injectivity follows easily from the equality $g\circ g=cos$ and noting that *cos* is a bijection from $[0;\frac{\pi}{2}]$ to $[0;1]$ we must have (classic) from the equality $g\circ g=cos$ the injectivity of g over $[0;\frac{\pi}{2}]$ (and the surjectivity of g as well over [0;1]).

Lemma. *Let $I\subset\mathbb{R}$ be a connected set (equivalently, I is an interval, that is, $\forall x,y\in I,\ [x,y]\cup[y,x]\subset I$). Let $h:I\to\mathbb{R}$ be an injective continuous function. Then h is strictly monotone.*

Proof. We define the set of ordered pairs from the domain I as follows:

$$D={<_{I\times I}}=\{(x,y)\in I\times I\mid x<y\}\subset I\times I.$$

Since I is an interval, the set D is convex. Indeed, let $A=(x_1,y_1)$ and $B=(x_2,y_2)$ be points in D, and let $\lambda\in[0,1]$. Since $x_1<y_1$, $x_2<y_2$, and $\lambda,1-\lambda\geq0$, the convex combination satisfies

$$\lambda x_1+(1-\lambda)x_2<\lambda y_1+(1-\lambda)y_2.$$

Moreover, since I is an interval, equivalently a convex set, we have

$$\lambda x_1 + (1-\lambda)x_2 \in I \quad \text{and} \quad \lambda y_1 + (1-\lambda)y_2 \in I.$$

Thus, $\lambda A + (1-\lambda)B \in D$, and hence D is convex. In particular, D is path-connected and therefore connected.

We now define a difference function $g : D \to \mathbb{R}$ by

$$g(x,y) = h(y) - h(x).$$

Since h is continuous on I, the function g is continuous on D, being the composition

$$D \xhookrightarrow{\iota} I \times I \xrightarrow{h\times h} \mathbb{R}\times\mathbb{R} \xrightarrow{-} \mathbb{R}.$$

Moreover, since h is injective, the function g never vanishes, that is, $0 \notin g[D]$. Recall that the image of a connected set under a continuous map is connected; therefore, $g[D]$ is a connected subset of $\mathbb{R}$, hence an interval. Consequently,

$$g[D] \subset \mathbb{R}_{>0},$$

in which case h is strictly increasing, or

$$g[D] \subset \mathbb{R}_{<0},$$

in which case h is strictly decreasing. This concludes the proof. □

-Now we can prove the result: we argue by contradiction. Let us fix a real continuous function $f : (\mathbb{R}, \mathcal{T}_{\mathbb{R}}) \longrightarrow (\mathbb{R}, \mathcal{T}_{\mathbb{R}})$ with the property that $f \circ f = cos$. Then we know by our second result that $f(\alpha) = \alpha$ and $f|_{[0;\frac{\pi}{2}]}$ is an injection. Since f is continuous, $f|_{[0;\frac{\pi}{2}]}$ must be a continuous injection. By our third result $f|_{[0;\frac{\pi}{2}]}$ is strictly monotone. Since $f(\alpha) = \alpha \in]0;1[\subset [0;\frac{\pi}{2}]$, and $f|_{[0;\frac{\pi}{2}]}$ is continuous we have that $\alpha \in (f|_{[0;\frac{\pi}{2}]})^{-1}[]0;1[] =: U \in \mathcal{T}^{\mathbb{R}}_{[0;\frac{\pi}{2}]}$. In this case, the composition $f \circ f$ must be strictly increasing over U; for if $x, y \in U \subset [0;\frac{\pi}{2}]$ with $x < y$ then by construction of U we have $f(x), f(y) \in [0;\frac{\pi}{2}]$ (important). Now by the strict monotonicity of $f|_{[0;\frac{\pi}{2}]}$, we have two cases. If $f|_{[0;\frac{\pi}{2}]}$ is strictly increasing then $f(x) < f(y)$ so that again we have $f(f(x)) < f(f(y))$. If $f|_{[0;\frac{\pi}{2}]}$ is strictly decreasing then $f(x) > f(y)$ and so $f(f(x)) < f(f(y))$. In all case $(f \circ f)(x) < (f \circ f)(y)$. Therefore $cos|_U = (f \circ f)|_U$ is strictly increasing. This is a contradiction with the fact that cos is strictly decreasing over $[0;\frac{\pi}{2}] \supset U$ **if** U contains at least 2 elements. The latter is true: by construction U is of the form $[0;\frac{\pi}{2}] \cap V$ with V an open set of $\mathbb{R}$, in particular (and by construction of $\mathcal{T}_{\mathbb{R}}$) V contains a basis element (which is an open interval $]c,d[$ of positive length) containing α. Therefore:

$$\alpha \in]c,d[\cap]0;1[\subset]c,d[\cap[0;\frac{\pi}{2}] \subset U$$

so $\varnothing \subsetneq [\alpha; min\{d,1\}[\subset U$, and U necessarily contains infinitely many points.

Remark: If f were differentiable at $\alpha = f(\alpha)$, then the third part would be much easier. Indeed,

$$\begin{aligned} 0 \overset{\alpha\in]0,1[}{>} -\sin(\alpha) &= \left(\frac{\mathrm{d}}{\mathrm{d}x}\cos\right)(\alpha) = \left(\frac{\mathrm{d}}{\mathrm{d}x}(f\circ f)\right)(\alpha) \\ &= \left(\frac{\mathrm{d}}{\mathrm{d}x}f\right)(f(\alpha)) \cdot \left(\frac{\mathrm{d}}{\mathrm{d}x}f\right)(\alpha) = \left(\frac{\mathrm{d}}{\mathrm{d}x}f\right)(\alpha)^2 \geq 0, \end{aligned}$$

which is a contradiction.

Lemma. *Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. Suppose there exists a connected open set $U \subset \mathbb{R}$ such that $f|_U$ is strictly decreasing. If f has a unique fixed point $\alpha \in \mathbb{R}$ which in addition satisfies $\alpha \in U$, then there is no continuous function $g : \mathbb{R} \to \mathbb{R}$ such that $f = g \circ g$.*

Proof. Suppose, for contradiction, that there exists a continuous function $g : \mathbb{R} \to \mathbb{R}$ such that $g \circ g = f$. Consider the fixed point $\alpha \in U$. We have

$$g(\alpha) = g(f(\alpha)) = g(g(g(\alpha))) = f(g(\alpha)).$$

Thus $g(\alpha)$ is a fixed point of f, and by its uniqueness we obtain $g(\alpha) = \alpha \in U$. In particular, by continuity of g, there exists an open interval I with $\alpha \in I \subset U$ such that $g[I] \subset U$.

Now observe that since $f|_U = (g \circ g)|_U = g \circ (g|_U)$ is strictly decreasing, it is injective. Thus $g|_U$ is injective. Since g is continuous and injective on the connected set U, $g|_U$ must be strictly monotone, and hence $g|_I$ is also strictly monotone.

1. If $g|_I$ is strictly increasing, then $g|_U$ is strictly increasing (as $I \subset U$), and since $g[I] \subset U$ we have that $(g \circ g)|_I$ is strictly increasing.
2. If $g|_I$ is strictly decreasing, then $g|_U$ is strictly decreasing (as $I \subset U$), and since $g[I] \subset U$ we have that $(g \circ g)|_I$ is strictly increasing.

In all cases, $f|_I = (g \circ g)|_I$ must be strictly increasing. This contradicts the initial assumption that $f|_U$ is strictly decreasing, and hence that $f|_I$ is strictly decreasing: indeed, $\alpha \in I$ and I is an interval, hence I contains at least 2 elements (in fact uncountably many), which provide the intended contradiction[1]. Therefore, no such continuous g exists. □

Lemma. *Spas ? it would be nice if you could make a lemma where such a g exists (remember about your inductive construction) and try to optimize the assumptions on the function f for such a g to exists*

Lemma. *Let $f : \mathbb{R} \to \mathbb{R}$ be a strictly increasing continuous function. Suppose that on any interval (a, b) where a and b are adjacent fixed points (i.e., $f(a) = a$, $f(b) = b$ and $f(x) \neq x$ for $x \in (a, b)$), the function satisfies either $f(x) > x$ or $f(x) < x$. Then there exists a continuous strictly increasing function $g : \mathbb{R} \to \mathbb{R}$ such that $g \circ g = f$.*

Proof. Since f is strictly increasing we could consider $\pm\infty$ as fixed point. So there is always fixed point, We provide the construction for an interval (a, b) of fixed point $a < b$ where $f(x) > x$. The case for $f(x) < x$ is analogous, and the global function is formed by the union of such constructions and the identity on the set of fixed points.

1. **Fundamental Interval:** Pick an arbitrary point $x_0 \in (a, b)$. Let $x_1 = f(x_0)$. Since $f(x) > x$, we have $x_0 < x_1$. We define the sequence $x_{n+1} = f(x_n)$ for all $n \in \mathbb{Z}$.
2. **Seed Map:** Choose a value c such that $x_0 < c < x_1$. Define g on the interval $[x_0, c]$ as any strictly increasing continuous function such that $g(x_0) = c$ and $g(c) = x_1$.
3. **Functional Extension:** For $x \in [c, x_1]$, we are forced by the requirement $g(g(x)) = f(x)$ to define:

   $$g(x) = f(g^{-1}(x))$$

   Because $g : [x_0, c] \to [c, x_1]$ is a bijection, g^{-1} is well-defined. This defines g on the entire "fundamental interval" $[x_0, x_1]$.

[1] If $S \subseteq \mathbb{R}$ and $h : S \to \mathbb{R}$ is a function then: h is both strictly increasing and strictly decreasing if and only if $|S| \leq 1$

4. **Inductive Propagation:** We extend g to the rest of (a, b) using the identity:

$$g(x) = f(g(f^{-1}(x)))$$

If g is defined on $[x_n, x_{n+1}]$, this relation defines it on $[x_{n+1}, x_{n+2}]$. Since f and f^{-1} are continuous and strictly increasing, g remains continuous and strictly increasing across the nodes x_n.

5. **Boundary Conditions:** Set $g(a) = a$ and $g(b) = b$. Since $\lim_{n\to-\infty} x_n = a$ and $\lim_{n\to\infty} x_n = b$, the monotonic nature of the construction ensures continuity at the fixed points.

Thus, g is a continuous iterative square root of f. $\square$

Problem B4 (Putnam 2001)

Let S denote the set of rational numbers different from $\{-1, 0, 1\}$. Define $f : S \to S$ by $f(x) = x - \frac{1}{x}$. Prove or disprove that

$$\bigcap_{n=1}^{\infty} f^{(n)}(S) = \emptyset,$$

where $f^{(n)}$ denotes f composed with itself n times.

Solution:

The intersection is empty. To see this, analyze the behavior of denominators under iteration of f. Let $x = \frac{m}{n} \in S$, where m, n are coprime integers. Applying f:

$$f\left(\frac{m}{n}\right) = \frac{m}{n} - \frac{n}{m} = \frac{m^2 - n^2}{mn}.$$

Since $\gcd(m^2 - n^2, mn) = 1$ (as m, n are coprime: if $p \in \mathbb{P}$ is such that $p|_{\mathbb{Z}} mn$ and $p|_{\mathbb{Z}} m^2 + n^2$ then either $p|_{\mathbb{Z}} m$ which implies that $p|_{\mathbb{Z}} n^2$ so $p|_{\mathbb{Z}} n$, or $p|_{\mathbb{Z}} n$ which similarly implies $p|_{\mathbb{Z}} n$ in all case this implies $p \mid_{\mathbb{Z}} \gcd(m, n)$ a contradiction), we have that:

$$\frac{m^2 - n^2}{mn} = \frac{\operatorname{sign}(mn)(n^2 - m^2)}{|mn|}$$

is reduced. For $m \neq 1$, $|mn| \geq 2|n|$. If $m = 1$, then $f\left(\frac{1}{n}\right) = \frac{1-n^2}{n}$, and since $n \neq \pm 1$, the numerator satisfies $|1 - n^2| \geq 3$ and then .

Iterating f, the denominator grows at least exponentially. Specifically:

- For $x \in S$, if the denominator of $f^{(k)}(x)$ is d_k, then $d_{k+1} \geq 2d_k$.
- Thus, $d_k \geq 2^k d_0$, where d_0 is the initial denominator.

For any rational $x = \frac{a}{b}$ (in reduced form), choose k such that $2^k > b$. Then $d_k > b$, so $x \notin f^{(k)}(S)$. Hence, x cannot belong to $\bigcap_{n=1}^{\infty} f^{(n)}(S)$. Since x was arbitrary, the intersection is empty.

Problem (Reservoir Sampling, Jeffrey S. Vitter)

We have a finite linked list of elements, $x_0 \to x_1 \to \ldots \to x_n$, where $n \in \mathbb{N}$ is **unknown**. Starting at x_0, we have a pointer to x_1, which leads to x_2, and so on, until we reach the end of the linked list x_n. At each step of traversing the list, we cannot go back, but we are informed whether or not we have reached the end. We have enough memory to store at least one of any of the elements x_i ($0 \le i \le n$), but perhaps not more; in particular, we cannot simply store the entire list in an array (unless, of course, $n = 0$).

(a) How can we select uniformly at random an element in the linked list, if we are allowed to traverse it only once? More precisely, in the situation where the list can be traversed only once, design an algorithm with input the pointer to the head of the linked list x_0 which outputs an element of the linked list chosen uniformly at random[2] (i.e. with probability $\frac{1}{n+1}$).

(b) Why might solving this problem be useful in practice?

Solution:

(a) First, it is very important that we do not know n; otherwise, the solution is easy: select in advance an index i between 0 and n with equal probability $\frac{1}{n+1}$, traverse the list, and store the i-th element. The difficulty arises because we do not know the exact value of n in advance. Moreover, we also know that we cannot store the entire list in an array (unless $n = 0$) and choose uniformly one element from it once we reach the end.

We present the simplest version of the Reservoir Sampling algorithm, which belongs to the family of randomized algorithms for selecting a random sample, without replacement, of $k \ge 1$ items from a population of unknown size $n \ge k$ in a single pass over the items. Heuristically:

- Start by storing the first element, since with only one element it must be selected.
- As we traverse the list, each new element should have a chance to replace the currently stored element. The probability of replacing the stored element should decrease as we move further along the list, to ensure that earlier elements retain their fair share of being selected.
- Specifically, when we reach the i-th element, we replace the stored element with probability $\frac{1}{i+1}$. This balances the probabilities so that every element seen so far has the same chance (that is $\frac{1}{i+1}$) of being chosen.
- By continuing this process until the end of the list, we guarantee that each element has probability $1/(n+1)$ of being selected.

[2]We assume that one can generate potentially infinitely many independent uniform random numbers in the interval $[0, 1]$ so in particular one has a pseudo-random number generators that is a random number generators.

Pseudo-code: Reservoir Sampling on a Linked List

Algorithm 1 ReservoirSampling(x_0)

```
Input: pointer to the head x_0 of a finite linked list
Output: a uniformly random element from the linked list
store ← x_0                    ▷ initially store the first element with probability 1
current ← x_0
i ← 1
while current.next ≠ NULL do
    i ← i + 1
    u ← random_uniform[0,1]
    if u ≤ 1/i then
        store ← current.next
    end if
    current ← current.next
end while
return store
```

Termination: The algorithm terminates because it iterates through a finite linked list. The variable `current` starts at the head of the list, x_0, and moves to the next element in each iteration of the `while` loop. Since the list contains a finite number $n+1$ of elements and each `current.next` eventually becomes `NULL`, the `while` loop executes exactly n times. After reaching the last element, the loop condition `current.next` $\neq$ `NULL` fails, causing the loop to exit and the algorithm to return the stored element. Therefore, the algorithm always terminates after a finite number of steps.

Correctness: By induction on n, it is easy to see that each element x_i (for $0 \leq i \leq n$) in the linked list will pass, in order of increasing indices, exactly once through the variable `current`, that the variable `store` is updated at most once between each update of `current`, and that it will not be updated when `current` $\leftarrow x_n$. It thus suffices to show that for each $n \geq 0$, for each $0 \leq j \leq n$, when `current` $\leftarrow x_j$, the variable `store` contains an element selected uniformly at random among $x_0, \ldots, x_j$ (i.e. with probability $\frac{1}{j+1}$). Fix $n \geq 0$; we prove this by induction on j:

Base case: If $j = 0$, then when `current` $\leftarrow x_0$, the variable `store` necessarily contains x_0, which is thus selected with probability $1 = \frac{1}{0+1}$.

Inductive step: Assume that $0 < j+1 \leq n$ and that when the variable `current` $\leftarrow x_j$, the variable `store` contains an element selected uniformly at random among $x_0, \ldots, x_j$ (i.e. with probability $\frac{1}{j+1}$). We show that when the variable `current` $\leftarrow x_{j+1}$, the variable `store` contains an element selected uniformly at random among $x_0, \ldots, x_{j+1}$ (i.e. with probability $\frac{1}{(j+1)+1}$).

Assume `current` $\leftarrow x_{j+1}$. This means that we entered the loop of the `while` instruction after `current` $\leftarrow x_j$ and at this time `current.next` is x_{j+1}. In this loop:

- We generate a number u uniformly at random in $]0,1[$ and store x_{j+1} in the variable `store` if $u \leq \frac{1}{(j+1)+1} \leq \frac{1}{2}$. Thus x_{j+1} is stored with probability $\frac{1}{(j+1)+1}$.
- For any previous element x_k with $0 \leq k \leq j$, the probability that it remains in `store` is

the probability it was already stored ($\frac{1}{j+1}$ by the inductive hypothesis) *and* that it is not replaced by x_{j+1}. Since all numbers are generated independently, this probability is

$$\frac{1}{j+1} \cdot \left(1 - \frac{1}{j+2}\right) = \frac{1}{j+1} \cdot \frac{j+1}{j+2} = \frac{1}{j+2}.$$

Hence, when `current` $\leftarrow x_{j+1}$ (so at the end of this loop), the variable `store` contains an element selected uniformly at random among $x_0, \ldots, x_{j+1}$ (with probability $\frac{1}{(j+1)+1}$). This concludes the induction step.

(b) This problem is useful in practice because it models situations where data arrive sequentially, and it is impossible or inefficient to store all elements at once. For instance, in streaming algorithms, online data processing, or when sampling from large files or network logs, *reservoir sampling* enables the selection of a uniformly random element using only constant memory and a single pass through the data.

Problem (Hongler)

Let U be a domain such that $U \supseteq \mathbb{D}$ and f a holomorphic function $U \to \mathbb{C}$. Show that if $f(\partial\mathbb{D}) = \gamma$ is a simple loop and $f|_{\partial\mathbb{D}} : \partial\mathbb{D} \to \gamma$ is injective, then $f|_{\mathbb{D}}$ is injective.

Solution: