Specialist English: Assignment 4

Rebecca J. Stones
rebecca.stones82@nbjl.nankai.edu.cn

Date due: 30 October 2017

This fourth assignment (worth 5% of the final mark) looks at optimizing the writing in a longer English-language snippet.

I'll scale the marks on this assignment according to $m \mapsto \min(m, 10)$ for Master's students and $m \mapsto \lceil m/1.3 \rceil$ for Ph.D. students.

My marking will be affected by (a) your English writing, (b) your LaTeX typesetting, (c) your mathematical presentation, and (d) your understanding of the underlying computer science. Basically, I will "peer review" your assignments.

Problem 1 We'll go through this snippet in some detail:

> **Random permutation:** Random permutation function is well studied in Combinatorial mathematics and group theory. In Cauchy's two-line notation, there are the preimage elements in the first row, and the image elements of the preimage elements in the second row. The random permutation function can be expressed as:
>
> $$\pi : \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix} \tag{2}$$
>
> where $\pi(i) = p_i (i = 1, \cdots, n)$. We define π^{-1} as the inverse function of π. When the condition satisfies $\pi(i) = i$, the permutation is called identical permutation denoted by I. The description of random permutation generation is as follows:
>
> **Algorithm 1** Random Permutation generation
>
> 1: set $\pi = I$
> 2: **for** $i = n : 2$ **do**
> 3: select a random integer j where $1 \leq j \leq n$;
> 4: swap $\pi(i)$ and $\pi(j)$;
> 5: **end for**

(Source: S. Fu, Y. Yu, M. Xu, *A Secure Algorithm for Outsourcing Matrix Multiplication Computation in the Cloud*, Proc. ACM Security in Cloud Computing, 2017.
dx.doi.org/10.1145/3055259.3055263
dl.acm.org/citation.cfm?doid=3055259.3055263

1. Why is it improper to say "random permutation function" above? [1 mark]
2. Which words are mistakenly capitalized? [1 mark]
3. What are the "preimage elements", the "image elements", and the "image elements of the preimage elements" of a permutation of $\{1, \ldots, n\}$? So what does the sentence beginning "In Cauchy's two-line notation ..." literally mean? [1 mark]
4. Rewrite "... where $\pi(i) = p_i(i = 1, \cdots, n)$" to be more (humanly) readable and technically correct. [1 mark]

5. How can we eliminate the notation p_i from the sentence beginning "The random permutation function ..."? (Hint: Look how Wikipedia[1] did it.) [1 mark]

6. Why is I a poor choice of notation for the identity permutation? [1 mark]

   (I recommend "id" (typeset `$\mathrm{id}$`) as the notation is self explanatory.)

7. Where do the authors actually define the term "random permutation"? [1 mark]

8. For each sentence in the snippet and for Algorithm 1, identify how it helps the reader understand the rest of the paper (if at all). [4 marks]

   - You'll need to download and look at the paper.
   - We can assume the reader has taken an undergraduate course in computer science or something equivalent.
   - We can assume the reader has access to the Internet.

9. Using at most one sentence, rewrite the snippet to give only the information identified in part 8. It needs to be grammatically correct and succinct. [2 marks]

[1] `https://en.wikipedia.org/wiki/Permutation#Definition_and_notations`