These notes are to answer the questions in the Ježil-Narusevych solution of Problem 4 (file Pr4.pdf).

**Q1 (Axiom of Choice)**: If $f : [x+1] \to [x]$ violates PHP then you can define $g : [x] \to [x+1]$ by:

$$g(y) = z \Leftrightarrow_{df} (y \in rng(f) \wedge f(z) = y) \vee (y \notin rng(f) \wedge z = 0)$$

which will be surjective (because $dom(f) = [x+1]$).

On the other hand, having surjective $g : [x] \to [x+1]$ define $f : [x+1] \to [x]$ by:

$$f(y) = z \Leftrightarrow_{df} (g(z) = y \wedge \forall z' < z g(z') \neq y) \ .$$

In other words, we replace AC by choosing in each $g^{-1}(y)$ the minimal element.

In fact, this is similar to why AC holds in Gödel's constructible universe: the choice function uses the order in which sets are introduced.

The name *dual (W)PHP* (denoted dWPHP) is actually the official name of the principle (no surjection from a set onto a proper superset) and it plays important role in bounded arithmetic (for formalizing probabilistic constructions) and in proof complexity (to define hard tautologies).

There is one subtle issue in the equivalence proof of PHP and dPHP above: the second definition involves a quantifier. That is, if you restrict PHP and dPHP to the class of, say, p-time functions then the proof of the equivalence of the two principles no longer holds and is probably not true. Note that the inverse function to a p-time function may not be p-time (e.g. factoring) itself.

**Q2:** I think (*) is not true: e.g. $|2| = |3| = 2$ (it is the bit length). But more importantly, even if it were true, your induction argument would need a statement of the form

$$\exists \text{ map } g : [x + 1 - t] \to \dots$$

for $t = 0, 1, \dots$ and this statement is not bounded: the code of a map $g : [x+1] \to [x]$ is like that of a sequence of length $x + 1$ of numbers $< x$ and may have size $\sim x^x$ which you cannot bound by a term.

Sooner or later we shall learn about theories allowing to quantify over functions with bounded domain and range but $I\Delta_0$ does not allow that.

**Q3:** This is OK. Let me just mention an alternative way (although essentially equivalent). First shorten $J$ to $J_1$:

$$x \in J_1 \Leftrightarrow_{df} \exists y < a, \ y \in J \wedge x = |y|$$

i.e. $J_1$ is something like $\log(J)$. $J_1$ is closed under successor because $J$ is closed under multiplication by 2. Now shorten $J_1$ further to $J_2 \subseteq J_1$ closed under addition. And then do the same construction as for the case $2a$ vs. $a$ but *on exponents* $k$ in the sums of powers of two. I.e. each $2^k$ gets moved to something like $2^{k/2} = (2^k)^{1/2}$. Well, there are surely details to iron out.