Report Lab2

Group: sudo rm -rf

## 2.1 Implementation

* **Task 1:**
* **Task 2:** Implemented the random binning encoder and tested it.
* **Task 3:** Implemented a function to compute the hamming distance and the random binning decoder, cascaded it with the encoder and tested on the legitimate receiver achieving perfect reliablity
* **Task 4:** Generated the eavesdropper data, gathered the distribution of z assuming u uniform (indeed the sum of probability without normalization is 8), computed the joint probability between u and z and finally the mutual informaztion. Plotted all the conditional probabilities.
* **Task 5:**
* **Task 6:**
* **Task 7:** Implemented two function to modulate and demodulate the signal and then the awgn channel. Tested it on 7 different SNR
* **Task 8:**

## 2.2 Considerations and Remark

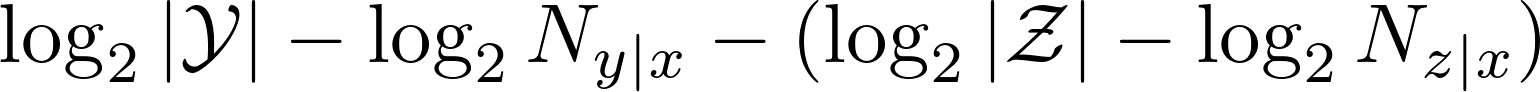
1. How many secret message bits per channel use (“transmitted word”) have you obtained with your scheme? **8**

How many secret bits per binary digits? **3**

2. Is it possible to obtain 4 secret bits per channel use? **NO**

If so, how should you change your encoder decoder? If not, why?

**Answer:** Since it is upperbounded to

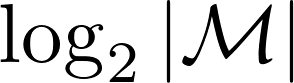


that in our case is equal to **3**

3. Is it possible to obtain 2 secret bits per channel use? **NO**

If so, how should you change your encoder decoder? If not, why?

**Answer:** Since it is lowerbounded to

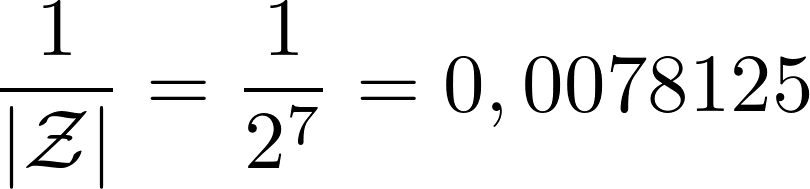


that in our case is equal to **3**

4. One could consider evaluating the secrecy of this mechanism by cascading the eavesdropper channel with a decoder and measuring the resulting error rates.

What do you expect the error rates should be?

**Answer:** We should achieve perfect secrecy and so the probability to guess u is



Why resort to (more complicated) evaluating the mutual information?

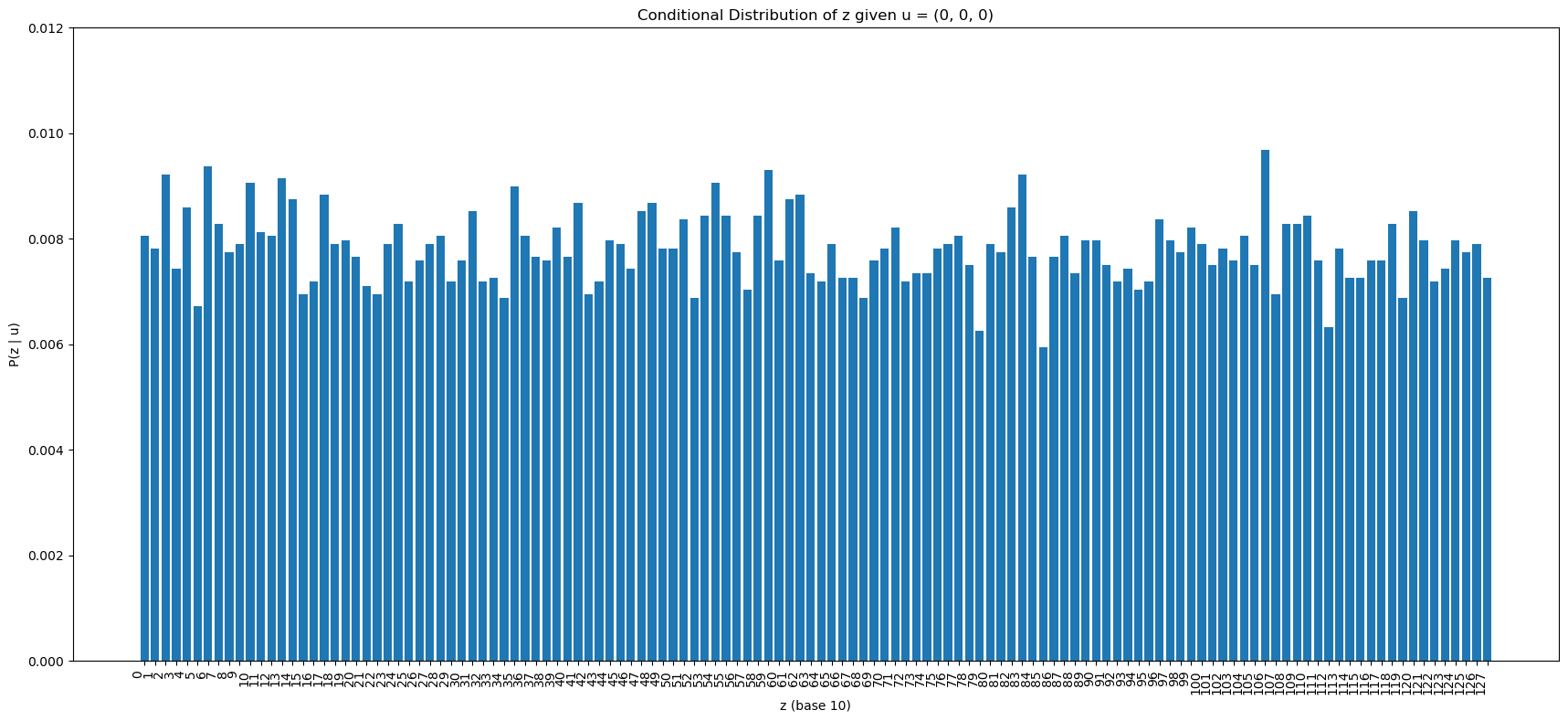
## 2.3 Evaluation of proper security metrics

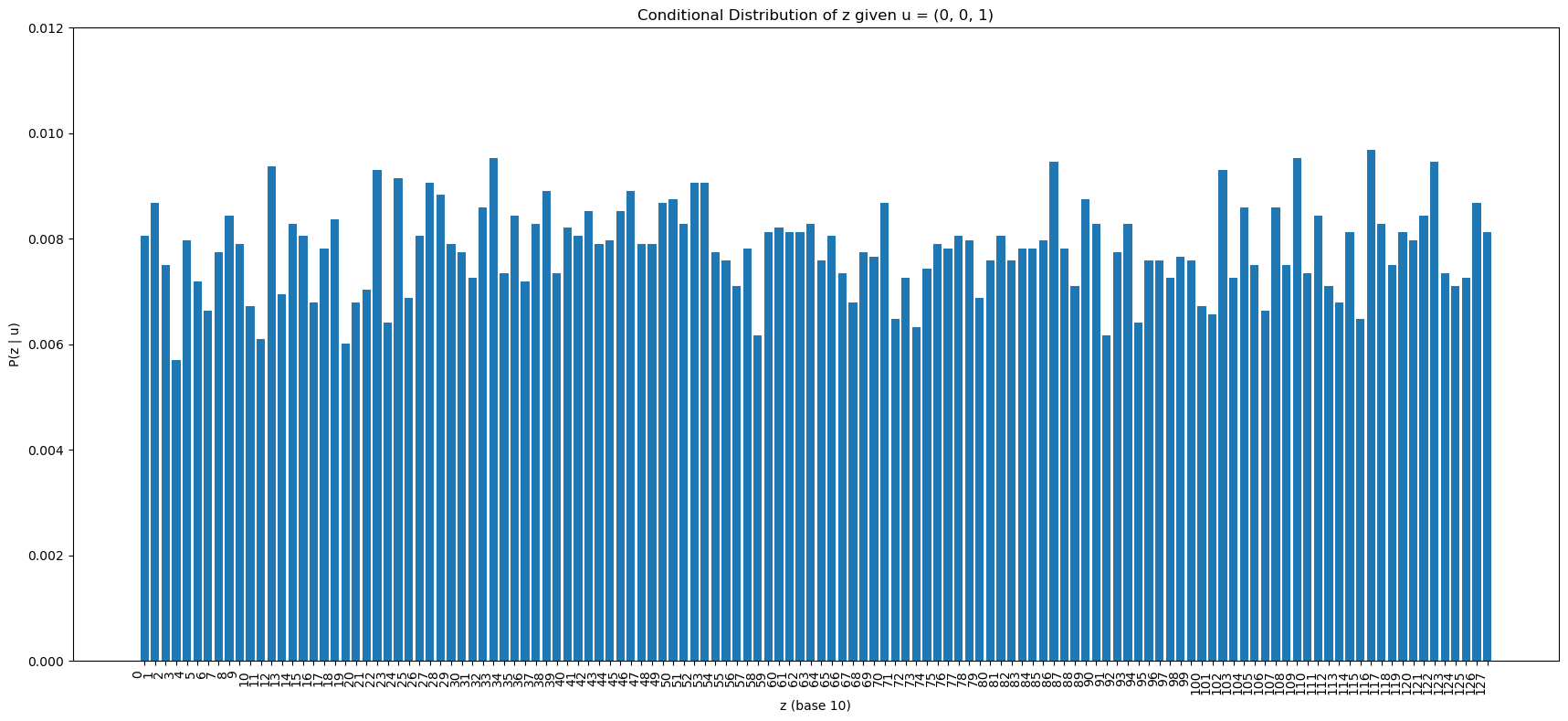
#### 1. plot of the conditional pmd from Task 1

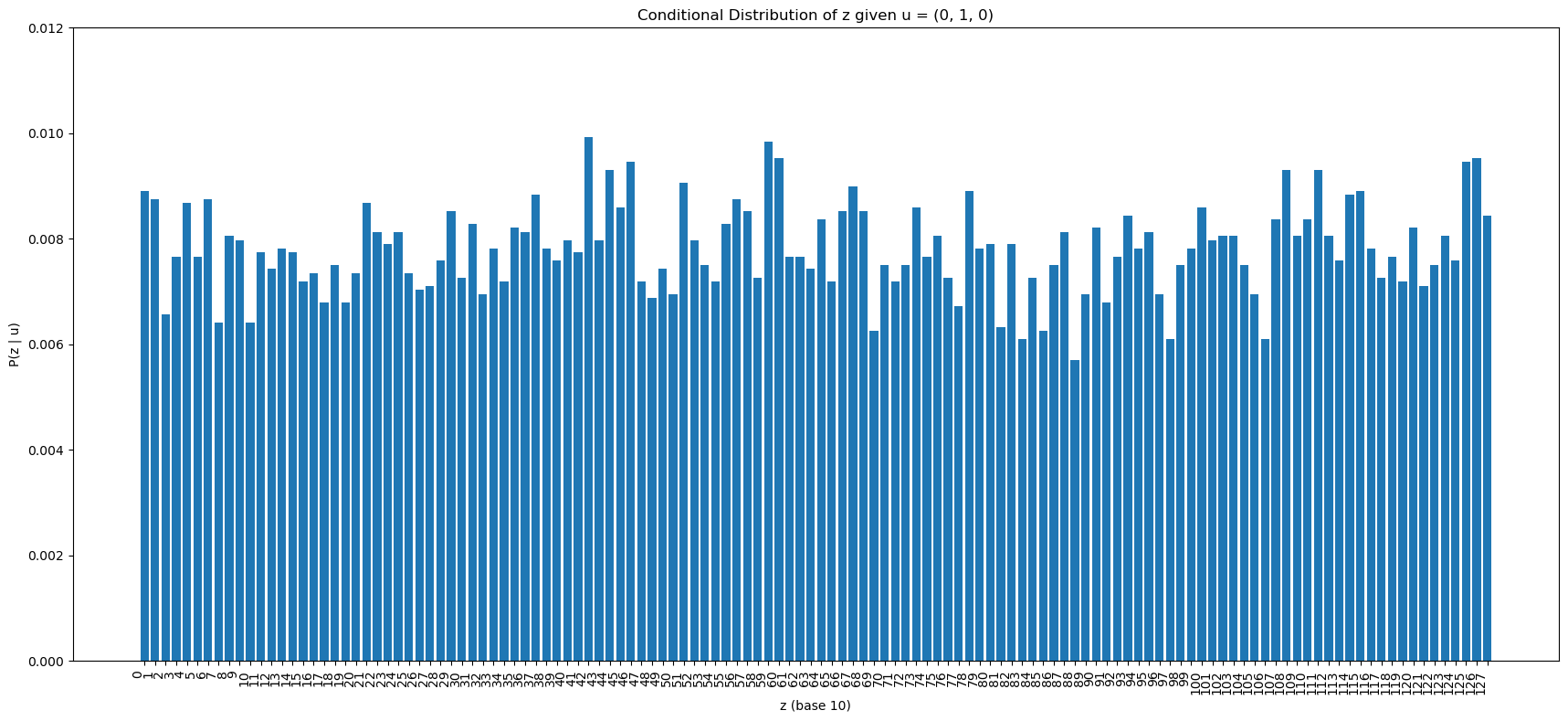


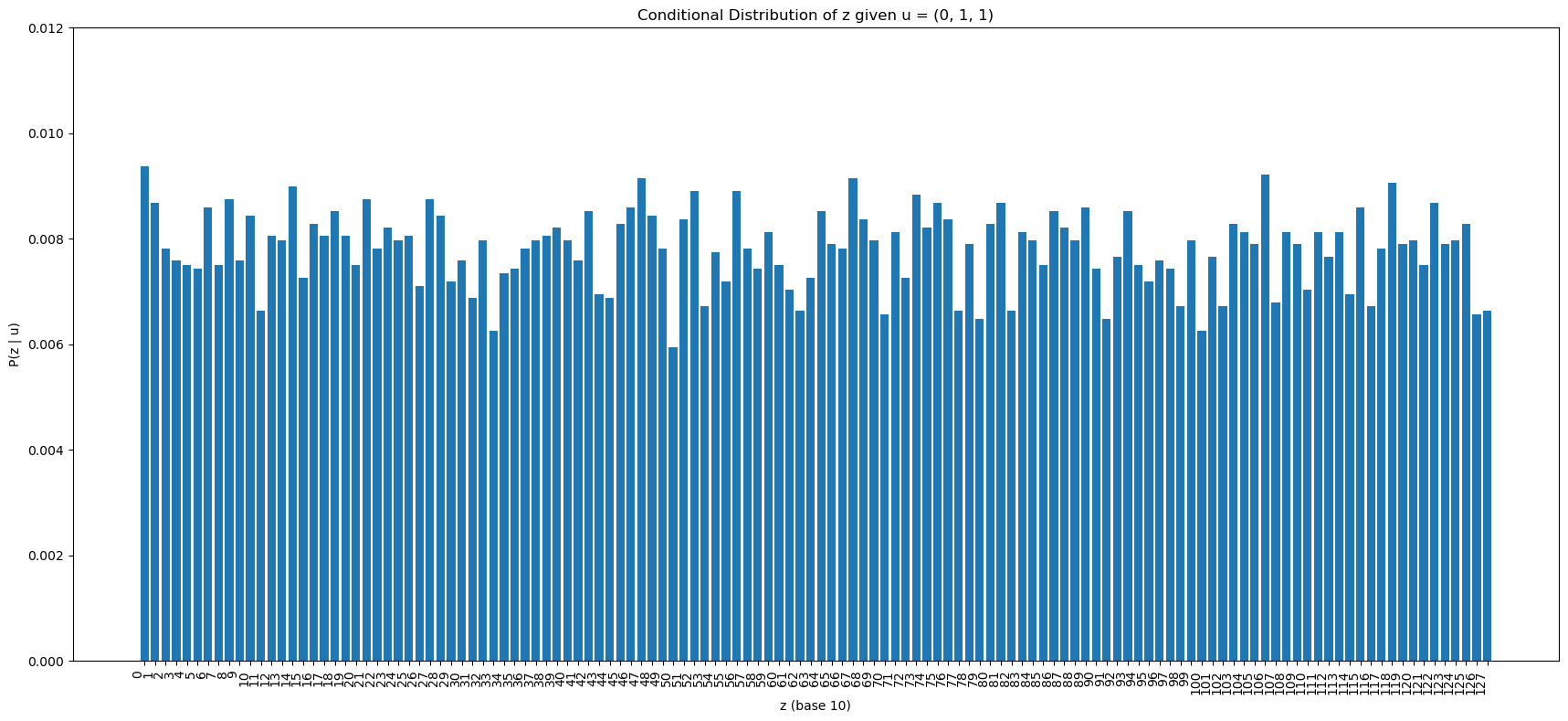
#### 2. plots of the conditional pmds for all values of d from Task 4

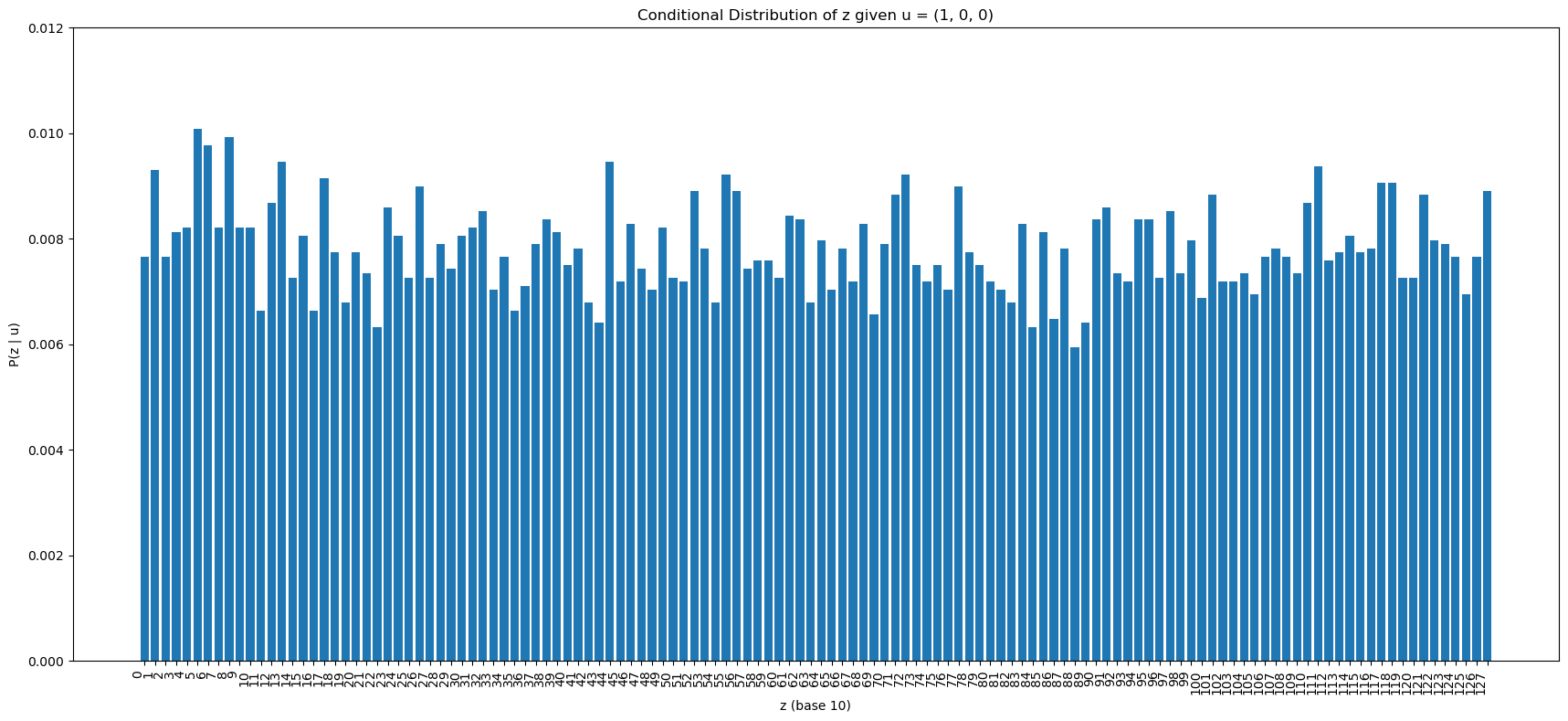


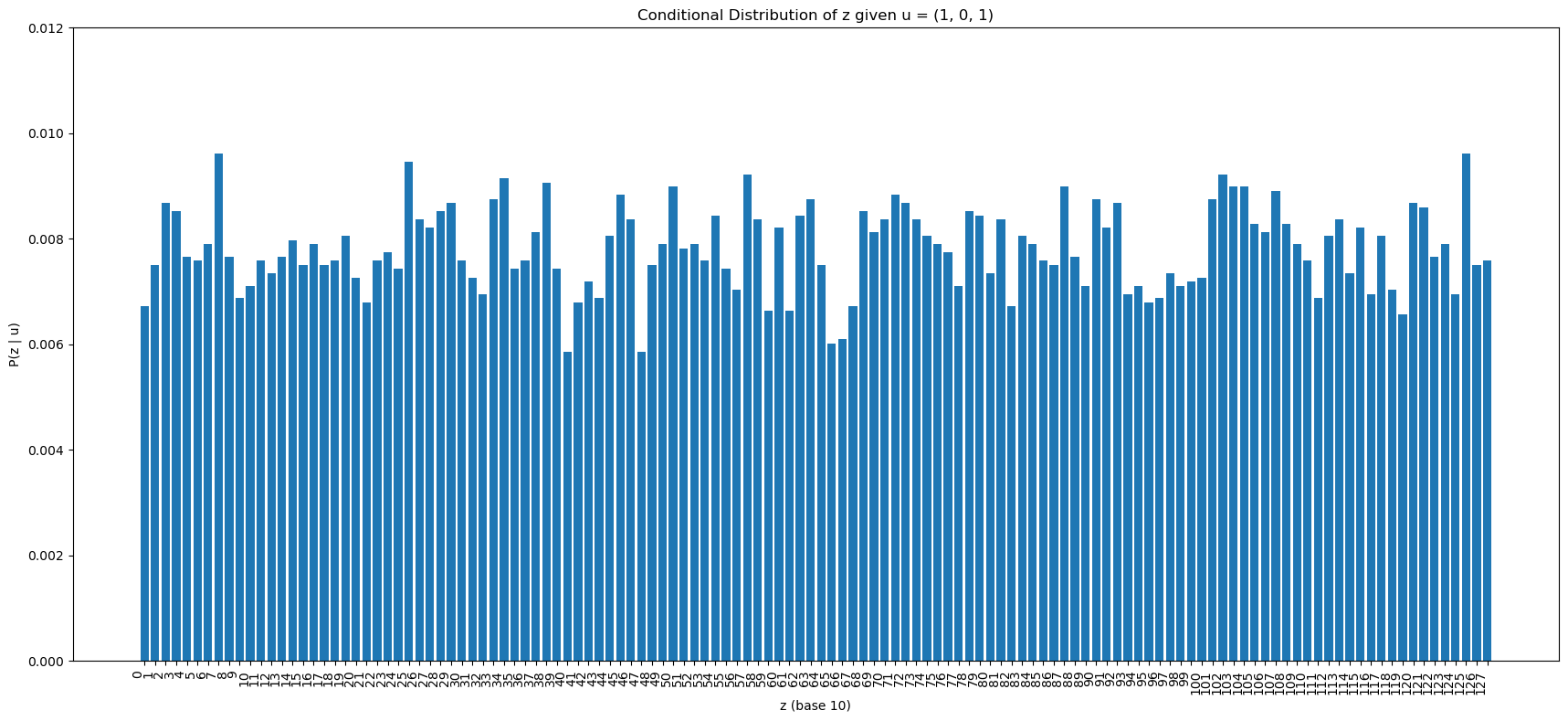












#### 

#### 

#### 3. Estimates of H(u), and I(u; z) from Task 4

I(u;z) = 0.006582

Since we found that u has uniform distribution

