[P16] We aim to prove that languages recognized by randomized Turing machines are contained in the second level of the polynomial hierarchy. More precisely: BPP$\subset \Sigma_2^p \cap \Pi_2^p$. (Intuitively, we have to show that the "expressive power" of "$\exists - \forall$-statements" is great enough to encode the statement that a BPP-machine will accept its input. That's conceptually not unlike e.g. the Cook-Levin proof about the expressiveness of Boolean formulas).

(1) In one sentence, why is it sufficient to establish that BPP$\subset \Sigma_2^p$?

(2) Let $L \in$BPP. I.e. there exists a TM M and a polynomial q such that

$$x \in L \quad \Rightarrow \quad \Pr_{r\in\{0,1\}^{q(|x|)}}[M(x,r)\,\text{accepts}] > 1-\delta \tag{1}$$

$$x \notin L \quad \Rightarrow \quad \Pr_{r\in\{0,1\}^{q(|x|)}}[M(x,r)\,\text{accepts}] < \delta. \tag{2}$$

In the definition of BPP, δ is chosen to be $1/3$. However, from sheet 4, we know that one can assume that $\delta = 2^{-|x|}$, which we will do from now on. Let $n = |x|$ be the length of the input and $m = q(|x|)$ the number of random bits. Let S_x be those random bits r for which M accepts the input pair $\langle x, r\rangle$. Re-formulate (1) and (2) as statements about the size $|S_x|$ of S_x.

(3) Let $k = \lceil \frac{m}{n} \rceil + 1$. The "$\exists - \forall$-statement" mentioned in the introduction will be:

$$\exists u_1, \ldots, u_k \{0,1\}^m \quad \text{such that}\, \forall r \in \{0,1\}^m : \, r \in \cup_{i=1}^k (S_x + u_i). \tag{3}$$

Here, $S_x + u_i$ is the set $\{s + u_i \,|\, s \in S_x\}$ where the addition of vectors in $\{0,1\}^m$ is element-wise and modulo 2. The easy direction is this: Show that if $x \notin L$ then $|S_x|$ is small enough that (3) is false.

(4) The slightly more difficult case consists in showing that if $x \in L$, then (3) is true. We need to show that there exists a choice $u_1, \ldots, u_k$ such that the union of the shifted sets $S_x + u_i$ equals all of $\{0,1\}^m$. The difficulty in proving the existence lies in the fact that we know nothing about the structure of S_x, other than a lower bound on its size. To anyway establish the existence claim, we employ the (fantastic!) *probabilistic method*: we'll prove that a *random* choice of u_i's has a non-zero chance of working. Hence there exists at least one working set of vectors (even if it remains totally unclear what that set might be).

So assume $x \in L$ and let the u_i be a uniformly drawn random vectors in $\{0,1\}^m$. Fix one $r \in \{0,1\}^m$. What is the probability that $r \notin (S_x + u_i)$ (Hint: $r + u_i$ is uniformly distributed)? From that, show that the probability that $r \notin \cup_{i=1}^k (S_x + u_i) \leq 2^{-nk} \leq 2^{-m}$ (Hint: use the fact that the u_i are independent). Use this in turn to prove that the probability that there exists *any* r such that $r \notin \cup_{i=1}^k (S_x + u_i)$ is smaller than one. (Hint: look up "union bound" or "Boole's inequality"). Complete the proof from here.

Note: The use of randomized arguments to prove a non-random statement ($x \in L \Rightarrow$ (3) true) may be surprising. It is, in fact, an *extremely* useful and fairly modern mathematical proof technique (going back to Erdősz). It pays to thoroughly understand and appreciate it! (8)