Quantum Computing

Mathias Niepert

Homework 6

Exercise 1

$0 < a < b$

- If $a \leq b/2$, then $b \bmod a < a \leq b/2$
- If $a > b/2$, then $b \bmod a = b - a < b/2$

$\Rightarrow$ In both cases $b \bmod a < b/2$.

Two division steps of the algorithm: (b, a) $\rightarrow$ (a, r) $\rightarrow$ $(r, a \bmod r)$ where $r = b \bmod a$.

Thus after two division steps b is replaced by something smaller than b/2 and after the first division step b is replaced by something smaller than a.

It follows that after at most $2log_2a + 1$ division steps, b is replaced by something smaller than 2 which causes the algorithm to stop.

Exercise 2

Let $b = b_{n-1}b_{n-2}...b_1b_0$ be a binary number ($b_i \in \{0, 1\}$). In the decimal system d(b) = $2(...(2(2b_{n-1} + b_{n-2}) + b_{n-3})...)) + b_0$

Thus: If $N = k * 2 + r$ with $r \in \{0, 1\}$, b_0 is r and $N^{(1)} = k$.

Next step: $N^{(1)} = k^{(1)} * 2 + r^{(1)}$, $b_1 = r^{(1)}$, $N^{(2)} = k^{(1)}$ and so forth. The algorithm terminates, if a $N^{(i)}$ is 0. More formal:
$b_0 = N \bmod 2 = r^{(1)}$
$b_1 = (N - r^{(1)})/2 \bmod 2 = r^{(2)}$, where $(N - r^{(1)})/2 = N^{(1)}$
$b_i = N^{(i)} \bmod 2$.

Exercise 3

(1) $\Sigma = \{0, 1\}$, $\Gamma = \{0, 1, \sqcup\}$, $Q = \{q_0\}$

δ :
$q_0 0 \rightarrow q_0 \sqcup R$
$q_0 1 \rightarrow q_0 \sqcup R$

(2) I program the TM to do 2 bit shifts to the right, which is a division by 4.

$\Sigma = \{0,1\}$, $\Gamma = \{0,1,\sqcup\}$, $Q = \{q_0, q_1, q_2, q_1', q_2', q_l\}$

δ :
$q_0\sqcup \rightarrow q_0 \sqcup R$ // if input is empty, never stop
$q_0 0 \rightarrow q_1 \sqcup R$
$q_0 1 \rightarrow q_2 \sqcup R$

$q_1 0 \rightarrow q_1 0 R$
$q_1 1 \rightarrow q_2 0 R$
$q_1 \sqcup \rightarrow q_l \sqcup L$

$q_2 0 \rightarrow q_1 1 R$
$q_2 1 \rightarrow q_2 1 R$
$q_2 \sqcup \rightarrow q_0 \sqcup R$

$q_l 0 \rightarrow q_l 0 L$
$q_l 1 \rightarrow q_l 1 L$
$q_l \sqcup \rightarrow q_1' 0 R$

$q_1' 0 \rightarrow q_1' 0 R$
$q_1' 1 \rightarrow q_2' 0 R$

$q_2' 0 \rightarrow q_1' 1 R$
$q_2' 1 \rightarrow q_2' 1 R$
$q_2' \sqcup \rightarrow q_0 \sqcup R$

(Tape at time t_0: $0^* b_{n-1} b_{n-2} ... b_0 \sqcup^\infty$.)

Exercise 4

The input string has length n. First of all the r/w head moves n+2 steps to write a blank at the beginning of the tape and b' at the end of the string. Then the head goes back to the beginning of the tape (n+1 steps). After this move it starts the "main" procedure (transitions 6-12):

1. Replace the i^{th} bit (starting with bit 1, not bit 0) with a blank and "save" this bit "in" the state r_b (1 step).

2. Move to the first blank (end of actual string on the tape). (n+1 steps).

3. Replace this blank with the "saved" i^{th} bit (1 step).

1-3 are done n-1 times.

If the head reaches b' (every bit of the input string has been duplicated) in the state q_1 go in the state q_{2+b} go to the beginning of the tape, replace the blank with 0 or 1 respectively (the very first bit of the string was "saved" in the bit b' and then in the state q_{2+b}) (n+1 steps). "Fall" over the tape and stop (1 step).

Overall we have $n+1+(n-1)(n+3)+n+1+1 = n^2+2n+2n+2+1-3 = n^2+4n$ steps. Thus, $t_m(n) = n^2+4n \in \mathbf{FP}$.