CS 181 HW 7

Call a verifier consistent proof system for QIS if you cannot prove a formula and its negation in F

That is, $\forall F, \neg(\exists S_1, S_2 (V(F, S_1) = 1) \wedge (V(NOT(F), S_2) = 1))$

Show that for every effective verifier V, there exists a QIS $C(V)$ that is true iff V is consistent.

Proof

① We are given the verifier V is consistent if $\forall$ formula F:
$\neg(\exists S_1, S_2 : (V(F, S_1) = 1) \wedge (V(NOT(F), S_2) = 1))$

② If V is effective, then there exists a QIS $C(V) = 1$ iff V is consistent.

③ We know that for all TM M which is input machine for HaltOnZero : $\exists$ QIS $R(M)$: $R(M) =$ True iff M halts on 0.

④ This means given a effective verifier V, we need to design a machine M that halt on 0 when V is consistent. We can write it as follows:

V is consistent implies that M halt on 0.

⑤ It means we need to find a formula F and 2 proofs which are S_1 & S_2 which could make the following statements holds:

$V(F, S_1) = 1$ & $V(NOT(F), S_2) = 1$

⑥ This is the structure of the machine M:

for (F, S_1, S_2) in $\{0,1\}^* \times \{0,1\}^* \times \{0,1\}^*$:

  if$(Eval(V, F, S_1) \wedge Eval(V, NOT(F), S_2))$:

    Halt

⑦ Note: We can write $\{0,1\}^* \times \{0,1\}^* \times \{0,1\}^*$ because the rotation is countable due to the fact that cartesian product of countable sets is countable. There is a way to enumerate all of the elements to avoid stuck in the infinite loop.

⑧ If it is consistent, either one of the Eval will be 0, so it means we only halt when there is inconsistency.

⑨ This means $R(M) = $ True imply M halt which then imply V is not consistent.

⑩ This is saying V is consistent refers to

$NOT(R(M)) = $ True

∎

Problem 2

Write a QIS for "There are infinitely many primes of the form $2^{2^k}+1$"

Answer

According to in class lemma, If $F(m,n)$ is a formula, Then $F_*(m,n)$ can be written as formula. Here is how the $F_*(m,n)$ should be define in terms of definition:

$$F_*(m,n) = \begin{cases} 1 & \text{if } \exists \text{ a finite sequence } m_1, m_2, \ldots, m_{k-1} \\ & \text{such that } F(m,m_1) = F(m_1,m_2) = \ldots = \\ & F(m_{k-1}, n) = 1 \\ 0 & \text{else} \end{cases}$$

$$\underbrace{m \quad m_1}_{F} \underbrace{\quad m_2}_{F} \cdots\cdots \underbrace{\quad n}_{F}$$

Here are some number to first recognize the pattern :

$F_0 = 2^1 + 1 = 3$

$F_1 = 2^2 + 1 = 5$

$F_2 = 2^4 + 1 = 17$

$F_3 = 2^8 + 1 = 257$

$F_4 = 2^{16} + 1 = 65537$

$\vdots$

$F_n = F_0 \cdot F_1 \cdot F_2 \ldots F_{n-1} + 2$ → I need to write the .... to a form accept by QIS

$F_3 = F_0 \cdot F_1 \cdot F_2 + 2 = (3 \times 5 \times 17) + 2 = 257$ } example for F_n

$$F(m,n) = \text{Multiply}(a,b) = \begin{cases} 1 & \text{if } a \times b \\ 0 & \text{else} \end{cases}$$

$$F_*(m,n) = \text{Multiply}_*(a,b) = \begin{cases} 1 & a \times \overbrace{C_1 \times C_2 \ldots \times C_K}^{\text{a chain of number multiply in between}} \times b \\ 0 & \text{else} \end{cases}$$

Multiply (a, C_1), Multiply (C_1, C_2), ..., Multiply (C_K, b)

$$\underbrace{\boxed{F_n = F_*(m,n) + 2}}_{\text{Multiply}_*(a,b)}$$

For this problem in particular :

We can define a chain of relationships :

If $F(m,n) : n = y \times m$

Then $F_*(1,n) : n = y \times 1$

If $m = 2$ & $y = 2$, n is a power of 2

$F_*(m,n) : n = ((m \times y) \times y) \times y \ldots$