پاسخ Research assignment

در ابتدا مفروضات ذکر شده به صورت رسمی را در نظر می‌گیریم.

مفروضات

(1) $\xrightarrow{R_M} M$

(2) $\xrightarrow{R_{AHE}} AHE$

(3) $\xrightarrow{P_{Pub}} TA$

(4) $M \underset{y_M}{\overset{y_{AHE}}{\rightleftharpoons}} AHE$

(5) $M \Longrightarrow a$

(6) $AHE \Longrightarrow b$

(7) $M \models \#(a)$

(8) $AHE \models \#(b)$

(9) $M \models AHE \Longrightarrow M \xleftrightarrow{K} AHE$

(10) $AHE \models M \Longrightarrow M \xleftrightarrow{K} AHE$

احکام

(11) $M \not\models AHE \xleftrightarrow{K} M$

(12) $AHE \models AHE \xleftrightarrow{K} M$

(13) $M \models AHE \models M \xleftrightarrow{K} AHE$

(14) $AHE \models M \models M \xleftrightarrow{K} AHE$

اثبات:

در ابتدا به سراغ حکم (11) می‌رویم. برای اثبات حکم (11) یا همان $M \models AHE \xleftrightarrow{K} M$ مطابق با گزاره‌ی مندرج در صفحه‌ی 5 مقاله کد در بخش Meter داریم check $M_1 = M_1'$ می‌باشد که برای اثبات باید ثابت کنیم $M \models M_1$ و نیز $M \models M_1'$ و در اینصورت است که Meter می‌تواند به نتیجه‌ی $M \models (M_1 = M_1')$ برسد و در نتیجه به $M \models AHE \xleftrightarrow{K} M$ خواهد رسید

حال بزار اثبات موارد مذکور ابتدا به سراغ $M E M'$ می‌رویم و پس $M E M_1$ را اثبات کرده و در نهایت به حکم شماره ۱۱ می‌رسیم.

طبق فرض

$$M \in ID_M \quad , \quad M \in (y_M = H_2(ID_M, y_{AHE})) \quad , \quad M \in y_{AHE}$$

نتیجه ① $M \in y_M$

نشان دادیم تا این لحظه که M به y_M باور دارد و از طرفی می‌دانیم که M ، r_M را کنترل می‌کند یا به عبارتی $M \Rightarrow r_M$ پس لذا چون متغیر خودش است آن را باور دارد یعنی $M \in r_M$.

با توجه به موارد فوق و نیز گزاره‌ی $S_M = r_M + y_M$ داریم:

$$M \in (S_M = r_M + y_M) \quad , \quad M \in r_M \quad , \quad M \in y_M$$

(با توجه به $M \Rightarrow r_M$)

نتیجه ② $M \in S_M$

تا این لحظه نشان دادیم که $M \in S_M$. از طرفی با توجه به آنکه M متغیر a را می‌سازد یا به عبارتی $M \Rightarrow a$ را می‌دانیم نتیجه بگیریم که $M \in a$ لذا تا این لحظه این دو عبارت مهم یعنی $M \in a$ و نیز $M \in S_M$ را در نظر می‌گیریم و به سراغ عبارت بعدی می‌رویم. بزار عبارت بعدی $M \in K$ داریم:

$$\frac{M \in K}{M \in k_{AHE \to M}}$$

از طرفی با در نظر گرفتن فرض ۹ در صورت نیاز و نیز عبارت بالا داریم:

فرض ۹ ↓ ، عبارت فوق

$$M \in AHE \Rightarrow (M \overset{K}{\longleftrightarrow} AHE) \; ; \; M \in k_{AHE \to M} \; , \; M \in ID_M \; , \; M \in T_{M'} \; , \; M \in y_{AHE} \; , \; M \in P_{Pub}$$

$$M \in T_x \; , \; M \in T_{AHE}$$

نتیجه ③

با توجه به فرمول مورد پذیرش بین دو طرف و مندرج در مقاله بالا $k_{AHE \to M}$

ادامه در صفحه بعد

حال با توجه به اثبات هایی که داشتیم و نتایجی که در ② و ③ و ④ اثبات کردیم، داریم:

$$\frac{M \in S_M \;,\; M \in T_{AHE} \;,\; M \in a \;,\; M \in (K_{M \to AHE} = (S_M + a) T_{AHE})}{\Rightarrow \text{نتیجه}\quad \underbrace{M \in K_{M \to AHE}}_{⑤}}$$

حال با در نظر گرفتن نتیجه فوق و مراجعه مجدد به پروتکل مندرج در مقاله داریم:

$$\frac{⑤\quad M \in K_{M \to AHE} \;,\; M \in (M'_1 = H_1(0, K_{M \to AHE}))}{\Rightarrow \text{نتیجه}\quad \boxed{M \in M'_1}} \qquad \text{مقاله}$$

تا این لحظه نشان دادیم که $M \in M'_1$ برقرار است. حال به سراغ اثبات $M \in M_1$ می رویم:

$$\frac{\xrightarrow{\text{فرض}} P_{pub} \to TA}{M \in P_{pub}}$$

از طرفی با توجه به فرض ۴ که $M \overset{y_{AHE}}{\underset{y_M}{\rightleftharpoons}} AHE$ می توانیم نتیجه بگیریم که $M \in y_{AHE}$.

از طرفی با روند اثباتی که در انتهای صفحه ۲ ذیل عبارت ③ داشتیم دیدیم که $M \in k_{AHE \to M}$ و نیز مفروضات مساله و پروتکلی که ذیل محاسبه $k_{AHE \to M}$ فوق‌لی ما ارائه کرده بود نتیجه گرفتیم که $M \in T_x$

و نهایتاً با توجه به آن مطالب و نتایج فوق داریم:

$$\frac{M \in T'_M \;,\; M \in T_x \;,\; M \in ID_M \;,\; M \in P_{pub} \;,\; M \in \#(a) \;,\; M \in (T_M = AP) \;,\; M \in (A = a + \%_1) \;,\; M \in y_{AHE}}{\Rightarrow \text{نتیجه}\quad \boxed{M \in M_1}}$$

حال که $M \in M_1$ و نیز $M \in M'_1$ داریم:

$$\frac{M \in M_1 \;,\; M \in M_2}{\Rightarrow \text{نتیجه}\quad \frac{M \in (M_1 = M_2)}{\Rightarrow \text{نتیجه}\quad M \in (AHE \overset{K}{\longleftrightarrow} M)}} \Rightarrow \boxed{M \in (AHE \overset{K}{\longleftrightarrow} M)}$$

اثبات حکم (11)

گام بعدی به سراغ اثبات حکم (12) می‌رویم و روند زیر را برای اثبات اتخاذ می‌کنیم:

ابتدا از فرض ۴ مندرج در راهنمایی مساله داریم:

$$\frac{M \overset{y_{AHE}}{\underset{y_M}{\rightleftharpoons}} AHE}{AHE \in y_{AHE}} \quad (6)$$

همچنین با فرض ۵ مندرج در راهنمایی مساله داریم:

$$\frac{\xrightarrow{P_{pub}} \boxed{TA} \}\rightarrow AHE \in P_{pub}}{} \quad (7)$$

و همچنین:

$$\frac{AHE \in r_{AHE} \;,\; AHE \in b \;,\; AHE \in (T_x = b + r_{AHE})}{AHE \in T_x} \quad (8)$$

($AHE \Rightarrow b$ طبق متاله)

حال باید ثابت کنیم که AHE به T_M هم وارد دارد تا نهایتاً با توجه به اینکه $AHE \in ID_M$ (9) بتوانیم از قوه حل $K_{AHE \to M} = T_x (T_M + H_2(ID_M, y_{AHE}) P_{pub})$ استفاده کنیم. لذا با توجه به فرض ۱ داریم که AHE باید به $k_{M \to AHE}$ وارد داشته باشد پس:

با توجه فرض ↓

$$\frac{AHE \in k_{M \to AHE} \;,\; AHE \in (K_{M \to AHE} = (S_M + a) T_{AHE})}{AHE \in S_M \;,\; AHE \in a \;,\; AHE \in T_{AHE}}$$

حال با توجه به عبارات بدست آمده در فوق داریم:

$$\frac{\xrightarrow{R_M} M \;,\; AHE \in a \;,\; AHE \in (A = a + r_M)}{AHE \in A}$$

ادامه مطلب بعد

حال که ثابت کردیم $AHE \in A$ می‌توانیم بگوییم توجه کنید که P متعلق به AHE است.

$$\frac{AHE \in A \;,\; AHE \in (T'_M = AP)}{AHE \in T'_M}$$

(۱۳)

حال با توجه به تابیع ④ و ⑦ و ⑧ و ⑨ و ⑩ می‌توانیم بگوییم:

$$AHE \in T'_M \;,\; AHE \in y_{AHE} \;,\; AHE \in ID_M \;,\; AHE \in r_{AHE} \;,\; AHE \in S_M \;,\; AHE \in T_x \;,\; AHE \in H(6)$$
$$AHE \in P_{Pub} \;,\; AHE \in (T_x = b + r_{AHE}) \;,\; AHE \in (k_{AHE \to M} =$$

فرمول متناله

$$k_{AHE \to M} = T_x\,(T'_M + H_2(ID_M, y_{AHE}) \times P_{Pub})$$

نتیجه $\Rightarrow AHE \in k_{AHE \to M}$

نهایتاً با توجه به عبارت فوق می‌توانیم بگوییم:

$$\frac{AHE \in k_{AHE \to M} \;,\; AHE \in (M'_2 = H_1(1, k_{AHE \to M}))}{AHE \in M'_2}$$

تا این لحظه ثابت کردیم که $AHE \in M'_2$. حال باید برایم $AHE \in M_2$ بروم. لذا این روند را آنجا ادامه می‌دهیم که:

با توجه به فرض ۱۰

$$\frac{AHE \in k_{M \to AHE} \;,\; AHE \in (M_2 = H_1(1, k_{M \to AHE}))}{\to AHE \in M_2}$$

نهایتاً داریم:

$$\frac{AHE \in M_2 \;,\; AHE \in M'_2}{\text{نتیجه} \to AHE \in (M_2 = M'_2)}$$

$$\text{نتیجه} \to AHE \in (AHE \xleftrightarrow{K} M)$$

$$\Rightarrow AHE \in (AHE \xleftrightarrow{K} M)$$

↑ اثبات حکم (12)

ادامه صفحه بعد

اکنون با توجه به اثباتی که بر حکم (11) (goal 1) و نیز حکم (12) (goal 2) انجام دادیم به راحتی می‌توانیم ۲ هدف دیگر یعنی حکم (13) (goal 3) و حکم (14) (goal 4) را اثبات کنیم.

با توجه به قرض ۹ و اثباتی که بر حکم (11) داشتیم، حکم (13) را اثبات می‌کنیم:

قرض ۹ ، حکم (11) ⟹ نتیجه

$$M \Vdash (AHE \overset{K}{\longleftrightarrow} M) \quad , \quad M \Vdash (AHE \Rightarrow (M \overset{K}{\longleftrightarrow} AHE))$$

$$M \Vdash AHE \Vdash (M \overset{K}{\longleftrightarrow} AHE)$$

اثبات حکم 13 یا goal 3

و همچنین برای goal 4 روند شبیهی با روند فوق را اتخاذ می‌کنیم و داریم:

قرض 10 ، حکم (12) ⟹

$$AHE \Vdash (AHE \overset{K}{\longleftrightarrow} M) \quad , \quad AHE \Vdash (M \Rightarrow (M \overset{K}{\longleftrightarrow} AHE))$$

$$AHE \Vdash (M \Vdash (M \overset{K}{\longleftrightarrow} AHE))$$

اثبات حکم 14 یا goal 4

پایان

بدین