۱ جلسه‌ی سوم

همان طور که در جلسات قبل گفتیم هر گزاره‌ای را در منطق گزاره‌ها می‌توان به صورت $f(p_1, ..., p_n)$ تصور کرد که در آن $p_1, ..., p_n$ گزاره‌های اتمی هستند. برای مثال $f(p_1, \ldots, p_n) = p_1 \wedge \ldots \wedge p_n$ یگ گزاره در منطق گزاره‌هاست. همچنین گفتیم که برای هر گزاره‌ای درمنطق گزاره‌ها یک جدول ارزش در نظر می‌گیریم که ارزش آن گزاره را بر حسب ارزش اجزای آن مشخص می‌کند.

مثال ۱. جدول ارزش گزاره‌ی $p_1 \wedge \neg p_2$ به صورت زیر است.

p_1	p_2	$\neg p_2$	$\neg p_2 \wedge p_1$
۰	۱	۰	۰
۰	۰	۱	۰
۱	۱	۰	۰
۱	۰	۱	۱

یک سوال طبیعی این است که آیا برای هر جدول ارزش دلخواه، می‌توان گزاره‌ای یافت که آن جدول ارزش را داشته باشد؟ پاسخ این سوال مثبت است و در لم زیر بدان پرداخته شده است.

لم ۲. برای هر تابع $F : \{0, 1\}^n \to \{0, 1\}$ یک گزاره‌ی $f(p_1, ..., p_n)$ چنان یافت می‌شود که برای هر ارزیابی μ داشته باشیم

$$\mu(f(p_1, ..., p_n)) = F(\mu(p_1), ..., \mu(p_n)).$$

اثبات. فرض کنید $\{\mu_i | i \leq 2^n\}$ شمارشی از کُلِّ نگاشتهای ارزیابی (محدود شده به گزاره‌های اتمیِ $p_1, \ldots, p_n$) باشد. گزاره‌ی $f(p_1, \ldots, p_n)$ به صورت زیر، دارای ویژگی خواسته شده در لم است:

$$\bigvee_{\{i | F(\mu_i(p_1), ..., \mu_i(p_n)) = 1\}} \bigwedge_{j=1,...,n} Q_{ij}$$

که در آن

$$Q_{ij} = \begin{cases} p_j & \text{اگر } \mu_i(p_j) = 1 \\ \neg p_j & \text{اگر } \mu_i(p_j) = 0 \end{cases}$$

به بیان ساده‌تر، اگر یک جدول ارزش داشته باشیم و بخواهیم گزاره‌ای با آن جدول ارزش پیدا کنیم، کافی است «فصلِ» سطرهائی را در نظر بگیریم که در آنها ارزش گزاره یک شده است. همچنین در هر کدام از این سطرها، عطف گزاره‌های اتمی و نقیض آنها را متناسب با ارزش آن گزاره‌ی اتمی در آن سطر در نظر می‌گیریم. (برای متوجه شدن این جملات به مثال زیر توجه کنید). □

مثال ۳. گزاره‌ای پیدا کنید که جدول ارزش زیر را داشته باشد:

$p_{۱}$	$p_{۲}$	$p_{۳}$	$f(p_{۱}, p_{۲}, p_{۳})$
۰	۰	۰	۰
۰	۰	۱	۰
۰	۱	۰	۰
۰	۱	۱	۱
۱	۰	۰	۰
۱	۰	۱	۱
۱	۱	۰	۱
۱	۱	۱	۰

پاسخ. بنا به اثبات لم بالا گزاره‌ی مورد نظر به صورت زیر است:

$$f(p_{۱}, p_{۲}, p_{۳}) = (\neg p_{۱} \wedge p_{۲} \wedge p_{۳}) \vee (p_{۱} \wedge \neg p_{۲} \wedge p_{۳}) \vee (p_{۱} \wedge p_{۲} \wedge \neg p_{۳}).$$

□

دقت کنید که در ساخت گزاره‌ی بالا، از نمادهای $\neg$ $\wedge, \vee,$ استفاده کردیم. از این رو لم بالا را معمولاً بدین صورت بیان می‌کنند: مجموعه‌ی نمادهای منطقی $\{\neg$ $\wedge, \vee,\}$ کامل است؛ یعنی هر جدول ارزشی را می‌توان با استفاده از این نمادها تولید کرد.

تمرین ۱. نشان دهید مجموعه‌ی $\{\neg, \wedge\}$ از نمادها کامل است.

دقت کنید که برای پاسخ دادن به تمرین بالا، کافی است نشان دهید که نمادِ $\vee$ از نمادهای $\neg$ $\wedge,$ حاصل می‌شود.

تمرین ۲. اداتِ دوتایی $|$ (بخوانید ادات شفر) را به صورت زیر در نظر بگیرید: (جدول ارزش آن را بکشید)

$$p \mid q := \neg(p \wedge q)$$

نشان دهید ادات شفر کامل است.

تمرین ۳. نشان دهید ادات $\downarrow$ ،(بخوانید اداتِ نُرْ) تعریف شده در زیر، کامل است.

$$p \downarrow q := \neg(p \vee q)$$

(جدول ارزش آن را نیز بکشید.)

تمرین ۴. نشان دهید تنها ادوات دوتاییِ [1] کامل همان $|$ و $\downarrow$ هستند.

تمرین ۵ (مندلسون). فرض کنید که وارد شهری شده‌اید که هر یک از مردم آن یا همیشه راست می‌گوید یا همیشه دروغ، و تنها می‌تواند با بله و نه جواب دهد. سر یک دوراهی یکی از مردم شهر ایستاده است. چگونه می‌توانید با یک سوال راه درست را پیدا کنید؟

[1] یعنی ادواتی که دو گزاره‌ی اتمی در آنها به کار رفته است

تعریف ۴.

۱. گزاره‌ی $f(p_1, ..., p_n)$ را یک تاتولوژی [2] می‌خوانیم، هرگاه برای هر تابع ارزیابی $\mu : M \to \{0, 1\}$ داشته باشیم $\mu(f(p_1, ..., p_n)) = 1$. (به بیان دیگر، هرگاه در جدول ارزش این گزاره، در پایان هر سطر، ارزش ۱ داشته باشیم).

۲. دو گزاره‌ی ψ و φ را معادل می‌خوانیم و می‌نویسیم $\psi \equiv \varphi$ هرگاه $\psi \leftrightarrow \varphi$ یک تاتولوژی باشند(به بیان دیگر هرگاه جداول ارزش φ و ψ یکسان باشند.)

مثال ۵. چند تاتولوژی مهم را در زیر آورده‌ایم. سعی کنید تاتولوژی بودن آنها را با رسم جدول ارزش تحقیق کنید:

۱. $A \to (B \to A)$

۲. $A \wedge B \to A$

۳. $A \to A \vee B$

۴. $\neg\neg A \leftrightarrow A$

۵. $(A \to (B \to C)) \leftrightarrow ((A \to B) \to (A \to C))$

۶. $A \to (B \to A \wedge B)$

۷. $(A \to B) \to ((C \to B) \to (A \vee C \to B))$

۸. $((A \to B) \wedge (\neg A \to B)) \to B$

۹. $(A \vee B \to C) \to (A \to C \wedge B \to C)$

رابطه‌ی معادل بودن دو گزاره، $\equiv$، یک رابطه‌ی هم‌ارزی روی مجموعه‌ی همه‌ی گزاره‌ها، PR است. بنابراین PR توسط این رابطه افراز می‌شود. مجموعه‌ی افرازهای این رابطه را با $PR/_\equiv$ نشان می‌دهیم. به آسانی می‌توان تحقیق کرد که $(PR/_\equiv, \wedge, \vee, \neg, [p \wedge \neg p], [p \vee \neg p])$ تشکیل یک جبر بولی می‌دهد.(این جبر بولی را جبرِ لیندن‌باوم‌ــ تارسکی می‌نامیم).

دقت کنید که گزاره‌ی $p \vee \neg p$ همواره درست است (یعنی تاتولوژی است). گزاره‌ی $p_1 \wedge p_2$ گاهی درست و گاهی غلط است. به گزاره‌ای که حداقل با یک ارزیابی درست باشد، **ارضاشدنی** یا **سازگار** [3] می‌گوییم. مثلاً گزاره‌ی $p_1 \wedge p_2$ در صورتی که $\mu(p_1) = \mu(p_2) = 1$، دارای ارزش یک است؛ پس ارضاشدنی است. به گزاره‌ای که ارضا شدنی نباشد، یک گزاره‌ی تناقض‌آمیز (یا یک تناقض) می‌گوییم. برای مثال $p \wedge \neg p$ یک تناقض است.

همان طور که متوجه شده‌اید، بررسی این‌که آیا گزاره‌ی $f(p_1, ..., p_n)$ تاتولوژی است یا خیر نیاز به کشیدن یک جدول ارزش با 2^n سطر دارد. یک سوال مهم این است که آیا روشی سریع‌تر برای تشخیص تاتولوژی بودن یک گزاره وجود دارد یا خیر. این مسأله معادل با یک مسأله‌ی باز در ریاضی و علوم رایانه‌ی نظری، به نام مسأله‌ی P=NP است.

برای توضیح بیشتر درباره‌ی مسأله‌ی P=NP مثال زیر را در نظر بگیرید. اگر یک پاسخ برای یک جدول سودوکو به ما بدهند، تشخیص این که آیا این پاسخ درست یا غلط است، آسان است. برای این کار کافی است تک تکِ سطرها و ستونهای

[2] tautology

[3] satisfiable, consistent

پاسخ را چک کنیم و این کار زمان چندانی نمی‌برد. با این حال اگر یک جدول سودوکوی حل نشده به ما بدهند، حل کردنِ آن زمان زیادی می‌برد.

مسأله‌ی P=NP می‌پرسد که آیا هر مسأله‌ای که برای چک کردن درستی یک جواب از آن، یک الگوریتمِ سریع وجود دارد، برای حل آن نیز الگوریتمی سریع وجود دارد؟ منظور از یک الگوریتم سریع، الگوریتمی با زمان چندجمله‌ای است. فرض کنید $p(x)$ یک چندجمله‌ای باشد. می‌گوییم یک الگوریتم دارای زمان $p(x)$ است هرگاه برای هر ورودیِ به طولِ x حداکثر پس از $p(x)$ مرحله بایستد.

پروژه ۶. برای مطالعه‌ی بیشتر درباره‌ی مسأله‌ی P=NP منبع زیر را مطالعه بفرمائید.

the importance of P vs NP question, Stephen Cook.

از سرکار خانم زهرا شیروانیان، برای قبول زحمت تایپ این جلسه سپاسگزاری می‌کنم.