

Önermeler mantığındaki biçimsel kanıtlar

David Pierce

26 Aralık 2011, saat 11:48

Bu yazının ana kaynakları, Burris'in [1] ve Nesin'in [4] kitapları ve *Foundations of Mathematical Practice* (Eylül 2010) adlı notlarım. Bazı terimler, [2, 3] kaynaklarından alınmıştır.

İçindekiler

1	Önermeler	1
2	Doğruluk tabloları	2
3	Eşdeğerlik	6
4	Gerektirme	8
	Kaynaklar	13

1 Önermeler

Önerme, belli bir *durumda doğru* veya *yanlış* denebilen *cümledir*. Matematikte, durum çoğunlukla bir *yapıdır*. Örneğin, *her sayının tersi var* cümlesi, bir önermedir, ve bu önerme,

- $(\mathbb{N}, +)$ yapısında yanlış,
- $(\mathbb{Z}, +)$ yapısında doğru,
- (\mathbb{Z}, \cdot) yapısında yanlış,
- (\mathbb{Q}^+, \cdot) yapısında doğrudur. (Burada $\mathbb{Q}^+ = \{x : x \in \mathbb{Q} \wedge x > 0\}$.)

Belli bir durumda, bir önermenin **doğruluk değeri** vardır:

- önerme doğru ise, değeri 1;
- önerme yanlış ise, değeri 0'dır.

$\{0, 1\}$ kümesi için,

\mathbb{B}

harfini kullanalım. Önergeler için, P , Q , ve R gibi Latin harflerini kullanalım. Sonsuz tane önermemiz varsa, P_0 , P_1 , P_2 ve benzerlerini kullanabiliriz. Bir d durumunda, P önermesinin \mathbb{B} kümesindeki değeri olarak

$d(P)$

kullanılabilir. O zaman d , önermeler kümesinden \mathbb{B} kümesine bir fonksiyondur (dönüşümdür):

$d: \{\text{önergeler}\} \rightarrow \mathbb{B}$.

2 Doğruluk tabloları

Verilmiş önermelerden, **bağlaçlarla**, **bileşke önermeler** yapılabilir, ve onların değerleri, verilmiş önermelerin değerlerinden bulunabilir. Örneğin:

P ve Q ;
 P veya Q ;
 P ise Q ;
 P ancak ve ancak Q ;
 P değil.

(Dilbilgisinde, *ise* ve *değil*, bağlaç değildir; ama matematikte, öyle sayılabilir.) Bu örneklerde, sözcüklerin yerinde, kısaltma olarak, simgeler kullanılabilir:*

$P \wedge Q$
 $P \vee Q$
 $P \Rightarrow Q$
 $P \Leftrightarrow Q$
 $\neg P$

Yukarıdaki simgelere, **bağlayıcı** diyelim. Bileşke önermelerin farklı durumlardaki doğruluk değerleri, **doğruluk tablolarında**[†] gösterilebilir:

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
0	0	0	0	1	1
1	0	0	1	0	0
0	1	0	1	1	0
1	1	1	1	1	1

P	$\neg P$
0	1
1	0

* $P \wedge Q$ yerine, $P \& Q$; $P \Rightarrow Q$ yerine, $P \rightarrow Q$; $P \Leftrightarrow P$ yerine, $P \leftrightarrow Q$, yazılabilir.

[†]Veya doğruluk çizelgelerinde.

Mesela, ikinci satırdan, $d(P) = 1$ ve $d(Q) = 0$ ise, o zaman $d(P \Rightarrow Q) = 0$.

Doğruluk tabloları şöyle yazılabilir:

P	\wedge	Q	P	\vee	Q	P	\Rightarrow	Q	P	\Leftrightarrow	Q	
0	0	0	0	0	0	0	1	0	0	1	0	\neg
1	0	0	1	1	0	1	0	0	1	0	0	P
0	0	1	0	1	1	0	1	1	0	0	1	0
1	1	1	1	1	1	1	1	1	1	1	1	

Burada, bir önermenin değeri, önermenin bağlayıcısının altına yazılır.

Aslında, $P \Rightarrow Q$ gibi bir ifade gerçek bir önerme değildir; bir **önerme formülüdür**; ve P ve Q harfleri, **önerme değişkenleridir**. Değişkenlerin yerine gerçek önermeleri koyarsak, önerme formülü, bir önerme olur.

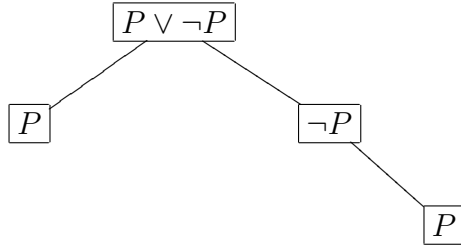
Bir önerme formülünde, birden fazla bağlayıcı kullanılabilir, mesela

$$P \vee \neg P$$

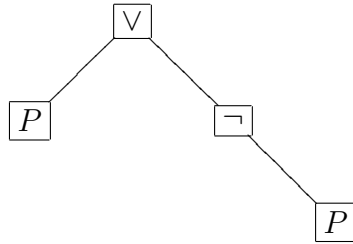
formülünde olduğu gibi. Bu formülün, üç veya dört tane **altformülü** var; bunlar

$$P \vee \neg P, \quad P, \quad \neg P, \quad P$$

formülleridir. Biz, P altformülünü tekrarladık, çünkü formülü bir **ağaç** şeklinde görebiliriz, ve bu ağacın dört tane **düğümü** olur:



Ağaçta, altformülün yerine, formülün **ana bağlayıcısını** koyabiliriz:

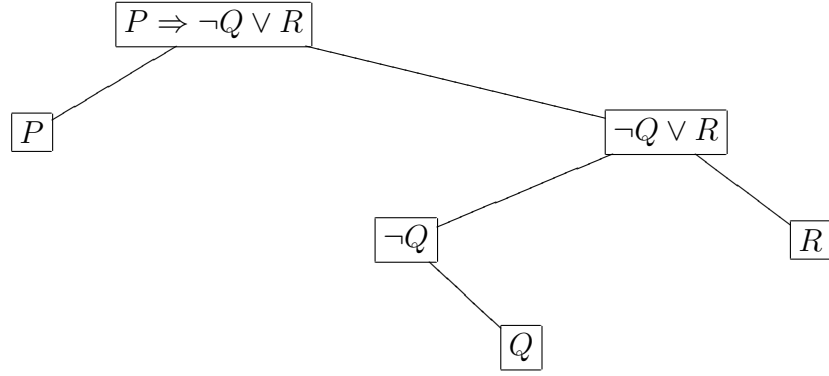


O zaman $P \vee \neg P$ formülün doğruluk tablosu iki şekilde yazılabilir:

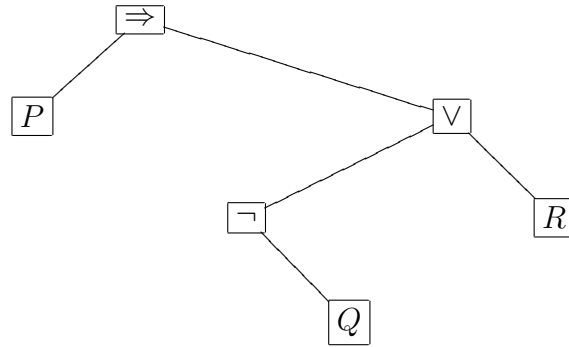
P	$\neg P$	$P \vee \neg P$	P	\vee	\neg	P
0	1	1	0	1	1	0
1	0	1	1	1	0	1

İkinci şekilde, her altformülün değeri, altformülün ana bağlayıcısının altına yazılır.

Bir örnek daha: $P \Rightarrow \neg Q \vee R$ (yani, $P \Rightarrow ((\neg Q) \vee R)$) önerme formülünün ağacı aşağıdadır:



Ana bağlayıcıları kullanarak,



şeklinde yazabiliriz. Doğruluk tablosu şöyle yazılabilir:

P	\Rightarrow	\neg	Q	\vee	R
0			0		0
1			0		0
0			1		0
1			1		0
0			0		1
1			0		1
0			1		1
1			1		1

P	\Rightarrow	\neg	Q	\vee	R
0		1	0		0
1		1	0		0
0		0	1		0
1		0	1		0
0		1	0		1
1		1	0		1
0		0	1		1
1		0	1		1

P	\Rightarrow	\neg	Q	\vee	R
0		1	0		1
1		1	0		1
0		0	1		0
1		0	1		0
0		1	0		1
1		1	0		1
0		0	1		1
1		0	1		1

ve sonunda,

P	\Rightarrow	\neg	Q	\vee	R
0	1	1	0	1	0
1	1	1	0	1	0
0	1	0	1	0	0
1	0	0	1	0	0
0	1	1	0	1	1
1	1	1	0	1	1
0	1	0	1	1	1
1	1	0	1	1	1

O zaman formülün **basit** doğruluk tablosu şöyledir:

P	Q	R	$P \Rightarrow \neg Q \vee R$
0	0	0	1
1	0	0	1
0	1	0	1
1	1	0	0
0	0	1	1
1	0	1	1
0	1	1	1
1	1	1	1

Genellikle doğruluk değerleri şu sırada hesaplanır:

1. \neg
2. \wedge ve \vee
3. \Rightarrow ve \Leftrightarrow
4. bir bağlayıcı iki kere kullanılmışsa, sağdaki.

Örneğin:

1. $P \Rightarrow Q \vee R$ demek $P \Rightarrow (Q \vee R)$;
2. $\neg P \wedge Q$ demek $(\neg P) \wedge Q$;
3. $P \wedge Q \vee R$ belirsiz;
4. $P \wedge Q \wedge R$ demek $P \wedge (Q \wedge R)$;
5. $P \wedge Q \wedge R \vee P$ belirsiz;
6. $P \Rightarrow Q \Rightarrow R$ demek $P \Rightarrow (Q \Rightarrow R)$;
7. $P \Rightarrow Q \wedge R \Rightarrow S$ demek $P \Rightarrow ((Q \wedge R) \Rightarrow S)$.

\wedge , \vee , \Rightarrow , \Leftrightarrow bağlayıcılarına **ikili** denir; \neg bağlayıcısına, **birli** denir. Ayrıca, 0 ve 1, **sıfırlı bağlayıcılar** olarak düşünülebilir.

Alıştırma 1. Aşağıdaki formülleri hesaplayın.

1. $1 \Rightarrow 1 \Rightarrow 1$,
2. $1 \Rightarrow 0 \Rightarrow 1$,

3. $(0 \Rightarrow 1) \Leftrightarrow 1$,
4. $(0 \Leftrightarrow 1) \Leftrightarrow (0 \Leftrightarrow 1)$,
5. $\neg\neg\neg 0$,
6. $(1 \vee 0) \wedge 0$,
7. $1 \vee (0 \wedge 0)$.

Alıştırma 2. Aşağıdaki formüllerin doğruluk tablolarını yapın:

1. $P \Rightarrow Q \Rightarrow P$;
2. $P \wedge Q \wedge R$;
3. $\neg(P \Leftrightarrow \neg(Q \Leftrightarrow R))$;
4. $(P \Rightarrow Q \vee R) \Rightarrow \neg P \vee Q$;
5. $(P \Rightarrow Q \vee \neg R) \wedge (Q \Rightarrow P \wedge R) \Rightarrow P \Rightarrow R$;
6. $\neg(\neg R \Rightarrow P \Rightarrow \neg(R \Rightarrow Q))$.

3 Eşdeğerlik

İki önermenin doğruluk değeri her durumda aynıysa, o önermeler, mantıksal olarak **eşdeğer** veya **denktir**. İki önerme *formülünün basit* doğruluk tabloları aynıysa, o formülleri de birbirine **eşdeğer** veya **denktir**. F ve G önerme formülleri eşdeğer ise,

$$F \sim G$$

ifadesini yazalım. Örneğin,

$$P \Rightarrow Q \sim \neg P \vee Q$$

denliğini aşağıdaki tablolardan görebiliriz:

$P \Rightarrow Q$	$\neg P \vee Q$
0 1 0	1 0 1 0
1 0 0	0 1 0 0
0 1 1	1 0 1 1
1 1 1	0 1 1 1

Buradan basit doğruluk tablolarının aynı olduğunu görürüz:

$P \quad Q \mid P \Rightarrow Q$	$P \quad Q \mid \neg P \vee Q$
0 0 1	0 0 1
1 0 0	1 0 0
0 1 1	0 1 1
1 1 1	1 1 1

Teorem 1. Aşağıdaki eşdeğerliklerimiz vardır.

1. (Her önerme, sadece \neg ve \wedge ile yazılabilir:)

$$\begin{aligned}P \vee Q &\sim \neg(\neg P \wedge \neg Q), \\P \Rightarrow Q &\sim \neg P \vee Q, \\P \Leftrightarrow Q &\sim (P \Rightarrow Q) \wedge (Q \Rightarrow P).\end{aligned}$$

2. (Her önerme, sadece \neg ve \Rightarrow ile yazılabilir:)

$$P \wedge Q \sim \neg(P \Rightarrow \neg Q).$$

3. (Çifte değilleme kaldırılabilir:)

$$\neg\neg P \sim P.$$

4. (De Morgan[‡] kuralları:)

$$\begin{aligned}\neg(P \vee Q) &\sim \neg P \wedge \neg Q, \\ \neg(P \wedge Q) &\sim \neg P \vee \neg Q.\end{aligned}$$

5. (\wedge ve \vee bağlayıcılarının değişme ve birleşme özellikleri:)

$$\begin{aligned}P \wedge Q &\sim Q \wedge P, & (P \wedge Q) \wedge R &\sim P \wedge (Q \wedge R), \\ P \vee Q &\sim Q \vee P, & (P \vee Q) \vee R &\sim P \vee (Q \vee R).\end{aligned}$$

6. (\wedge ve \vee bağlayıcıları birbirine üzerine dağılır:)

$$\begin{aligned}P \wedge (Q \vee R) &\sim (P \wedge Q) \vee (P \wedge R), \\ P \vee (Q \wedge R) &\sim (P \vee Q) \wedge (P \vee R).\end{aligned}$$

7. (Fazlalıklar:)

$$\begin{aligned}P \wedge P &\sim P, & P \wedge \neg P &\sim 0, & P \wedge 1 &\sim P, & P \wedge 0 &\sim 0, \\ P \vee P &\sim P, & P \vee \neg P &\sim 1, & P \vee 0 &\sim P, & P \vee 1 &\sim 1.\end{aligned}$$

8. (Yeni değişken:)

$$\begin{aligned}P &\sim (P \wedge Q) \vee (P \wedge \neg Q), \\ P &\sim (P \vee Q) \wedge (P \vee \neg Q).\end{aligned}$$

9. (Yutma:)

$$\begin{aligned}P \wedge (P \vee Q) &\sim P, \\ P \vee (P \wedge Q) &\sim P.\end{aligned}$$

Kanıt. Alıştırma. □

[‡]Augustus De Morgan, 1806–71, Büyük Britanyalı matematikçi ve mantıkçı [6, 5].

4 Gerektirme

Bir durum, bir önermeler kümesinin **modelidir**, eğer o durumda, kümenin her önermesi doğru ise. Eğer bir önerme, bir önermeler kümesinin her modelinde doğru ise, o küme, önermeyi **gerektirir**.

Γ (yani, *Gamma*), bir önerme formülü kümesi olsun, ve F , bir önerme formülü olsun. Eğer $\Gamma \cup \{F\}$ kümesindeki bütün formüllerin doğruluk tablosunun her satırında,

1. ya Γ kümesindeki bir formül yanlış ise,
2. ya da F formülü doğru ise,

o zaman Γ , F formülünü **gerektirir** deriz, ve

$$\Gamma \models F$$

ifadesini yazarız; \models simgesine, **turnike** denebilir. Boş küme, F formülünü gerektirirse,

$$\models F$$

yazılabilir, ve F formülüne **doğrusal geçerli formül**, veya **mantıksal doğru formül**, veya **totoloji** denebilir.

Teorem 2. $F \sim G$ ancak ve ancak $F \Leftrightarrow G$ bir totolojidir.

Kanıt. Alıştırma. □

Γ kümesinin F formülünü gerektirdiğini nasıl gösterebiliriz? İki yöntemimiz var:

1. doğruluk tabloları,
2. *biçimsel kanıt*.

Mesela, aşağıdaki tabloya bakın:

P	Q	$P \Rightarrow Q$	P	Q
0	0	1	0	0
1	0	0	1	0
0	1	1	0	1
1	1	1	1	1

Her satırda,

- ya $d(P \Rightarrow Q) = 0$ veya $d(P) = 0$,
- ya da $d(Q) = 1$.

O zaman

$$P \Rightarrow Q, P \models Q \quad (*)$$

(yani, $\{P \Rightarrow Q, P\} \models Q$).

Aynı şekilde,

$$P \vee Q \vee R, P \Rightarrow Q, Q \Rightarrow R \models R, \quad (\dagger)$$

çünkü, aşağıdaki doğruluk tablosundaki her satırda,

- ya $d(P \vee Q \vee R) = 0$, veya $d(P \Rightarrow Q) = 0$, veya $d(Q \Rightarrow R) = 0$,
- ya da $R = 1$.

(İkisi de olabilir, 6. satırdaki gibi.)

P	Q	R	$P \vee Q \vee R$	$P \Rightarrow Q$	$Q \Rightarrow R$	R
0	0	0	0	1	1	0
1	0	0	1	0	1	0
0	1	0	1	1	0	0
1	1	0	1	1	0	0
0	0	1	1	1	1	1
1	0	1	1	0	1	1
0	1	1	1	1	1	1
1	1	1	1	1	1	1

Ama şimdi

$$\Gamma = \{\neg(S \wedge T), (R \wedge Q) \vee (T \wedge Q), P \vee (S \wedge \neg T), \neg T \vee (Q \wedge (S \vee R)), \neg R \vee T\}$$

olsun. O zaman

$$\Gamma \models P \wedge Q \wedge R \wedge \neg S \wedge T; \quad (\ddagger)$$

ama bunu doğruluk tablolarıyla göstermek sıkıcı olurdu. *Biçimsel kanıt* yöntemi, bu durumda hem daha kısa, hem daha ilginçtir.

Biçimsel kanıt, bir formüller listesidir. F_0, F_1, \dots, F_n , bir biçimsel kanıt olsun. Her k için, $0 \leq k \leq n$ ise,

1. ya F_k , bilinen bir totolojidir,
2. ya bilinen bir gerektirmesine göre, $\{F_0, \dots, F_{k-1}\} \models F_k$,
3. ya da F_k , biçimsel kanıtın bir **hipotezidir**.

Kanıtın **sonucu**, F_n önerme formülüdür. Kanıtın hipotezleri, Γ kümesini oluştursun. O zaman Γ , F_n formülünü gerektirir:

$$\Gamma \models F_n.$$

Biçimsel kanıt, Γ 'dan F_n formülünü kanıtlar.

Bilinen bir totolojiye **aksiyom** denir. Başlangıçta, aksiyom olarak,

$$1, \quad P \vee \neg P$$

formüllerini, ve daha genellikle her $F \vee \neg F$ formülünü, kullanabiliriz. Başka bir formülü aksiyom olarak kullanmak istersek, kullanabiliriz, ama önce onun totoloji olduğunu ispatlamalıyız (mesela, doğruluk tablosuyla).

Bilinen bir gerektirmeye, **çıkarm kuralı** denir. Mesela, zaten (*) satırından

$$P \Rightarrow Q, P \models Q$$

gerektirmesini biliyoruz. O zaman, çıkarm kuralı olarak, **ayırma kuralımız**[§] var, yani: $P \Rightarrow Q$ ve P formüllerinden, Q çıkar. Daha genel olarak, $F \Rightarrow G$ ve F formüllerinden, G çıkar. Hatta daha genel olarak, $F \Rightarrow G$ ve F formülleri, Γ kümesinin öğeleriye, Γ kümesinden G çıkar.

Ayrıca, $F \sim G$ ise, o zaman

$$F \models G.$$

Teorem 1'den, bilinen denkliklerimiz var. O zaman şu çıkarm kuralımız var: Teorem 1'e göre, $F \sim G$ ise, ve F, Γ kümesinin öğesiye, o zaman G, Γ 'dan çıkar.

Örneğin, $P \wedge Q \models Q$, çünkü biçimsel bir kanıt yazabiliriz:

$$P \wedge Q, \quad 1, \quad \neg P \vee 1, \quad \neg P \vee \neg Q \vee Q, \quad \neg(P \wedge Q) \vee Q, \quad (P \wedge Q) \Rightarrow Q, \quad Q$$

Açıklamalarımızı eklersek:

(1)	$P \wedge Q$	[hipotez]
(2)	1	[aksiyom]
(3)	$\neg P \vee 1$	[2. satırdan, fazlalıkla]
(4)	$\neg P \vee \neg Q \vee Q$	[3. satırdan, fazlalıkla]
(5)	$\neg(P \wedge Q) \vee Q$	[4. satırdan, De Morgan kuralıyla]
(6)	$(P \wedge Q) \Rightarrow Q$	[5. satırdan]
(7)	Q	[1 & 6 satırından ayırma]

Ayrıca,

$$P \vee Q \vee R, \neg P, \neg Q \models R,$$

çünkü biçimsel bir kanıt yazabiliriz:

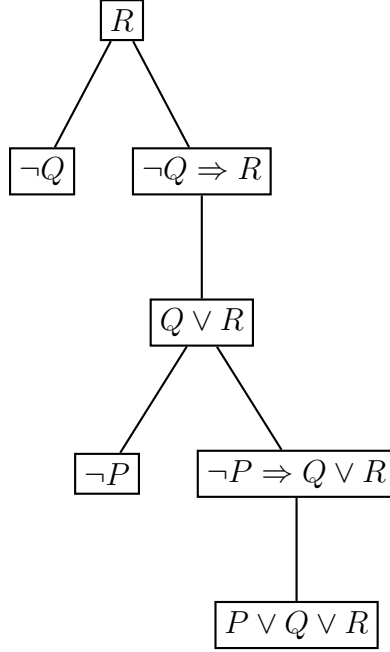
$$P \vee Q \vee R, \quad \neg P \Rightarrow Q \vee R, \quad \neg P, \quad Q \vee R, \quad \neg Q \Rightarrow R, \quad \neg Q, \quad R.$$

Açıklamalarımızı eklersek:

(1)	$P \vee Q \vee R$	[hipotez]
(2)	$\neg P \Rightarrow Q \vee R$	[1. satırdan]
(3)	$\neg P$	[hipotez]
(4)	$Q \vee R$	[2. ve 3. satırlardan, ayırma kuralıyla]
(5)	$\neg Q \Rightarrow R$	[4. satırdan]
(6)	$\neg Q$	[hipotez]
(7)	R	[5. ve 6. satırlardan]

[§]Bu kural, Latince *modus ponens*, İngilizcede, **detachment**.

Her biçimsel kanıtın arkasında, bir ağaç vardır. Mesela, son kanıtın ağacı şöyle:



Bu biçimsel kanıtın sıralanmasını değiştirebiliriz; örneğin, şöyle yazabiliriz:

$$\neg Q, \quad P \vee Q \vee R, \quad \neg P, \quad \neg P \Rightarrow Q \vee R, \quad Q \vee R, \quad \neg Q \Rightarrow R, \quad R.$$

Yeni çıkarım kuralları aşağıdaki teoremden gelir:

Teorem 3. *Bu gerektirmelerimiz var:*

1. (Basitleştirme:)

$$P \wedge Q \models P, \quad P \wedge Q \models Q.$$

2. (Ekleme:)

$$P \models P \vee Q, \quad Q \models P \vee Q.$$

3. (Bağlama:)

$$P, Q \models P \wedge Q.$$

4. (Ayrırma:)

$$\begin{array}{ll} P, P \Rightarrow Q \models Q, & P \vee Q, \neg P \models Q, \\ \neg Q, P \Rightarrow Q \models \neg P, & P \vee Q, \neg Q \models P. \end{array}$$

(hipotetik tasım:)

$$P \Rightarrow Q, Q \Rightarrow R \models P \Rightarrow R.$$

5. (Olumlu dilemma:)

$$P \Rightarrow Q, R \Rightarrow S, P \vee R \models Q \vee S.$$

Kanıt. Alıştırma. □

Şimdi yukarıdaki (†) gerektirmesininin bu biçimsel kanıtı var (her satırın nedeni nedir?):

$$\begin{array}{ll} P \vee Q \vee R & [\text{hipotez}] \\ (P \vee Q) \vee R & \\ \neg(P \vee Q) \Rightarrow R & \\ P \Rightarrow Q & [\text{hipotez}] \\ Q \Rightarrow R & [\text{hipotez}] \\ P \Rightarrow R & \\ P \vee Q \Rightarrow R \vee R & \\ P \vee Q \Rightarrow R & \\ (P \vee Q) \vee \neg(P \vee Q) \Rightarrow R \vee R & \\ (P \vee Q) \vee \neg(P \vee Q) & \\ R \vee R & \\ R. & \end{array}$$

Ayrıca, yukarıdaki (‡) gerektirmesininin, Tablo 1'deki biçimsel kanıtı var.

Alıştırma 3. Aşağıdaki gerektirmeler için biçimsel kanıtları yazın.

1. $\models P \Rightarrow P \Rightarrow P$
2. $\models P \Rightarrow Q \Rightarrow P$
3. $\models P \vee (P \Rightarrow Q)$
4. $\models (P \Rightarrow Q) \vee \neg Q$
5. $P \Rightarrow Q \wedge R \models P \Rightarrow Q$
6. $P \wedge \neg P \models Q$
7. $P \wedge (Q \vee R) \models P \Leftrightarrow (\neg Q \vee P)$
8. $P \Rightarrow Q, P \Rightarrow \neg Q \models \neg Q$
9. $P \Rightarrow R, Q \Rightarrow R \models P \vee Q \Rightarrow R$
10. $P \Rightarrow R, Q \Rightarrow S \models P \vee Q \Rightarrow R \vee S$

$(R \wedge Q) \vee (T \wedge Q)$ $(R \vee T) \wedge Q$ Q $R \vee T$ $\neg R \vee T$ $(R \vee T) \wedge (\neg R \vee T)$ $(R \wedge \neg R) \vee T$ $1 \vee T$ T $\neg(S \wedge T)$ $\neg S \vee \neg T$ $\neg\neg T$ $\neg S$	$\neg S \wedge T$ $P \vee (S \wedge \neg T)$ $\neg S \vee \neg\neg T$ $\neg(S \wedge \neg T)$ P $\neg T \vee (Q \wedge (S \vee R))$ $Q \wedge (S \vee R)$ $S \vee R$ R $R \wedge \neg S \wedge T$ $Q \wedge R \wedge \neg S \wedge T$ $P \wedge Q \wedge R \wedge \neg S \wedge T$
---	--

Tablo 1: Biçimsel bir kanıt

Kaynaklar

- [1] Stanley N. Burris, *Logic for mathematics and computer science*, Prentice Hall, Upper Saddle River, New Jersey, USA, 1998.
- [2] Abdurrahman Demirtaş, *Matematik sözlüğü*, Bilim Teknik Kültür Yayınları, Ankara, 1986.
- [3] Teo Grünberg and Adnan Onart, *Mantık terimleri sözlüğü*, Türk Dil Kurumu Yayınları, Ankara, 1976.
- [4] Ali Nesin, *Önermeler mantığı*, Bilgi Üniversitesi Yayınları, Ekim 2001.
- [5] Dirk Struik, *Kısa matematik tarihi*, Sarmal Yayınevi, İstanbul, 1996, Türkçesi: Yıldız Silier.
- [6] Dirk J. Struik, *A concise history of modern mathematics*, fourth revised ed., Dover, New York, 1987.