Ayrık Matematik
(Ayrık İşlemsel Yapılar)

Fırat İsmailoğlu, PhD

Hafta 4:
Kanıt ve Tümevarım I

Hafta 4
Plan

1. Bilgisayar bilimlerinde kanıtın önemi
2. Direkt kanit
3. Karsitters kanit
4. Olmayana ergi yöntemi ile kanit
5. Tumevarimla kanit

Kanıt (İspat) (Proof)

Kanıt : Bir iddianın gerçek olduğunu ortaya koyan *ikna edici* savdır (argümandır).

Burada ikna okuyucunuzun/dinleyicinizin kim olduğuna göre değişir. Yani kimin için ispat yaptığımız önemlidir. Buna göre çalişmamizi detaylandırırız.

ör. n ve k pozitif tamsayı ve $2 \leq k \leq n$ olsun. Bu durumda $n! + 1$ sayısı, k sayısına tam olarak bölünmez.

Kanit 1: $n! = 1 \cdot 2 \cdot \cdots \cdot k \cdot \cdots \cdot n$ tamsayısı k'ya tam olarak bölünür. $n!$'den sonra gelen k'ya tam olarak bölünen ilk tam sayı $n! + k$'dır. $k \geq 2$ olduğu için $n! < n! + 1 < n! + k$ olur. Şu halde $n! + 1$ sayısı, k sayısına tam olarak bölünmez.

Kanit 2: $\frac{n!+1}{k} = \frac{n!}{k} + \frac{1}{k} = \frac{1 \cdot 2 \cdots \cdot \cancel{k} \cdots \cdot n}{\cancel{k}} + \frac{1}{k} = m + \frac{1}{k}$. $(m \in \mathbb{Z}^{+})$ $\frac{1}{k}$ kalan olur, $n! + 1$ sayısı, k sayısına tam olarak bölünmez

Kanıtlar bilgisayar bilimlerinde neden gereklidir?

Kanitlar olası bugları önlemeye yardımcı olur. Yazdığınız bir algoritmanin gerçekten istediğiniz gibi çalıştığını anlamanız ve anlatmamız için bu algoritmanin çalıştığını ve çalışma süresini kanıtlamanız gerekir. ör jet motoru

Bir algoritmanın diğerinden üstünlüğünü (kompleksIik ve dogruluk bakımından) gösterebilmek icin yine kanitlara ihtiyacimiz vardir.

Yada çözmeye calıştiğimiz bir problemin çözülemez oldugunu gostermek icin kanita ihtiyacimiz vardir.

Algoritmalar formal matematiksel ifadelerdir, dolayisiyla kesin, belirisiz olmamasi gerekir. Bu kesinlik kanitlarla saglanir.

Kanıtlama Teknikleri

Kanıtlama teknikleri genel olarak 1. Direkt Kanitlama, 2. Karsitters (contrapositive) ile Kanitlama 3. Olmayana Ergi Yöntemi ile Kanitlama (Zıtlıkla Kanıtlama)

1. Direkt Kanit

Bir onermeyi direkt kanitlamak istiyorsak bilinen gerçek ve verilerden faydalanip surekli cikarim yaparak yeni gerçekler elde ederiz ve sonuca variriz.

ör. Bir n poizitif tamsayının 4'e tam bölünebilmesi icin son iki basamaginin 4'e bölünebilmesi gerekir.

Direkt Kanit: n sayısını basamaklarına ayıralım ($n = b_0 b_1 b_2 \ldots\ b_k$):

$$n = b_0 + 10b_1 + 100b_2 + \cdots + 10^k b_k$$

Eşitligin her iki tarafini 4'e bölelim:

$$n/4 = (b_0 + 10b_1)/4 + 25b_2 + \cdots + 25 \cdot 10^{k-2} b_k \qquad (*)$$

n'in 4'e tam bölünebilmesi demek $n/4$'un tam sayı olması demektir.

(*) eşıtliğinde, eşitligin sag tarafinin tam sayi olabilmesi icin $(b_0+10b_1)/4$ ün tam sayi olmasi gerekir (cunku kalan terimler zaten tam sayi), bu ise b_0+10b_1'in yani n sayisinin son iki basamaginin 4'e tam bölünebilir olmasini gerektir. $\square$

Not 1: Kanıtta kullandığımız $n \in \mathbb{Z}^+$, genel (generic) bir elemandir. Pozitif tam sayı olması disinda n ile ilgili hiç bir varsayım yapilmamistir. Böylece n için geçerli olan kanitimiz $\mathbb{Z}^+$'nin butun elemanlari icin de gecerli olur.

Not 2: Bu ispati yaparken kullandigimiz gercekler:

i) n'in 4'e tam bölünebilmesi $n/4$'un tam sayı olması anlamina gelir.

ii) a bir tamsayı iken $x+a$'nın bir tamsayi olabilmesi icin x de bir tam sayi olmalidir.

ispat yaparken bilinen gerçekleri kullanarak yeni gerçekler uretiyoruz!

Direkt kaniti $p \Rightarrow q$ formundaki onermeleri kanitlarkende kullaniriz. Burada p’nin dogru oldugunu varsayip q'nun dogru olduguna ulasirsak kaniti tamamlamis oluruz.

(Hatirlarsak p dogru iken $p \Rightarrow q$’nun dogru olmasi icin q dogru olmak zorundaydi, cunku p dogru iken q yanlissa $p \Rightarrow q$ yanlis olur).

ör. x ve y iki rasyonel sayi olsun. Bu durumda xy de rasyonel sayi olur.

$(x, y \in \mathbb{Q} \Rightarrow xy \in \mathbb{Q})$

Kanıt: $x, y \in \mathbb{Q}$ doğru olsun. Bu durumda vardir n_x, n_y, d_x ve d_y tamsayilari oyleki d_x ve d_y 0 dan farklidir ve $x = \frac{n_x}{d_x}$, $y = \frac{n_x}{d_x}$. Bu durumda $xy = \frac{n_x}{d_x} . \frac{n_y}{d_y} = \frac{n_x n_y}{d_x d_y}$ olur; öyleki $n_x n_y$, $d_x d_y$ tamsayi ve $d_x d_y$ 0’dan farklidir (cunku hem d_x hemde d_y 0 dan farkli). Sonuc olarak xy de rasyonel sayi olur. $\square$

$$\underbrace{(x, y \in \mathbb{Q}}_{\text{bilinen gerçek}} \Rightarrow \underbrace{\exists n_x, n_y, d_x \neq 0, d_y \neq 0 \in \mathbb{Z} \ni x = \frac{n_x}{d_x}, y = \frac{n_y}{d_y} \Rightarrow xy = \frac{n_x n_y}{d_x d_y}}_{\text{ortaya çıkan gerçekler}} \Rightarrow \underbrace{xy \in \mathbb{Q})}_{\text{sonuç}}$$

2. Karsitters (contrapositive) ile Kanıtlama

$p \Rightarrow q$ formundaki onermeleri ispatlarken bazen $p \Rightarrow q$ ya mantiksal olarak denk olan $\sim q \Rightarrow \sim p$ yi kanitlamak daha kolaydir. Eger $\neg q \Rightarrow \neg p$ yi kanitlarsak $p \Rightarrow q$'yu da kanitlamis oluruz.

ör. $x, y \in \mathbb{R}$ olsun. Eğer $|x| + |y| \neq |x + y|$ ise $xy < 0$.

Kanit:

$p = |x| + |y| \neq |x + y|$ ve $q = xy < 0$ olsun. $p \Rightarrow q$ ya denk olan $\sim q \Rightarrow \sim p$ nin dogru oldugunu kanitlayacagiz.

Su halde $\sim q \Rightarrow \sim p$: $\quad xy \geq 0 \Rightarrow |x| + |y| = |x + y|$

$xy \geq 0$ dogru oldugunu varsayalim. İki durum vardir.

1. durum: $x \geq 0$ ve $y \geq 0$. O halde $|x + y| = x + y = |x| + |y|$ olur.
2. durum: $x \leq 0$ ve $y \leq 0$. O halde $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$

İki durumda da $\sim q \Rightarrow \sim p$ dir. O halde $p \Rightarrow q$ olur. $\square$

ör. Bir tamsayinin çift olmasi icin gerek ve yeter şart sayinin karesinin çift olmasidir.

$(n \in \mathbb{Z}, \ n\, çift \Leftrightarrow n^2\, çift)$

Kanit:

$\Rightarrow$

$n\, çift \Rightarrow n^2\, çift$ oldugunu gosterecegiz. n çift ise vardir $k \in \mathbb{Z}$ öyleki $n = 2k$. Bu durumda $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. $2k^2 = l$ olsun. Bu bir tamsayidir. O halde $n^2 = 2l$ olup n^2 çifttir.

$(n\, çift \Rightarrow n = 2k, k \in \mathbb{Z} \Rightarrow n^2 = 4k^2 = 2(2k^2) \Rightarrow n^2 = 2l, l = 2k^2 \in \mathbb{Z} \Rightarrow n^2\, çift)$

$\Leftarrow$

$n^2\, çift \Rightarrow n\, çift$ oldugunu gosterecegiz. Bunu karsitters ile gosterelim: $n\, tek \Rightarrow n^2\, tek$.
$n\, tek \Rightarrow n = 2k + 1, k \in \mathbb{Z} \Rightarrow n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Sonuç olarak vardır bir $l = 2k^2 + 2k \in \mathbb{Z}$ öyleki $n^2 = 2l + 1$. O halde n^2 tektir. $n\, tek \Rightarrow n^2\, tek$ olduğunu ispatlamis olduk. Bu ise $n^2\, çift \Rightarrow n\, çift$ olmasina denktir. $\square$

3. Olmayana Ergi Yöntemi (OEY) (Zıtlıkla Kanıtlama)

Bir p önermesini kanıtlamaya çalışırken bazen bu önermenin tersinin (zıttının) doğru olduğunu varsayarız. Eğer bu varsayım elimizdeki gerçeklerle *çelişirse* önermenin tersinin yanlış olduğu böylece önermenin kendinin doğru olduğunu göstermiş oluruz.

(Kısaca OEY'de önermenin tersini kabul ettigimizde bir çelişki bulmamiz gerekir).

(Tersi yanlışsa kendi doğrudur)

ör. q: *asal sayılar sonsuzdur* önermesini OEY ile kanıtlayalım. Bu önermenin tersi $\sim q$: *asal sayılar sonludur* önermesi doğru olsun. O halde bir p_{en} asal sayısi vardır öyleki bu asal sayı en büyük asal sayıdır.

$k = 2 \times 3 \times \cdots \times p_{en} + 1$ şeklinde bir tamsayı oluşturalım. Kendinden ve 1 den başka tam sayı böleni olmadığından bu sayı da asaldır; üstelik bu sayı p_{en}'den büyüktür. Bu ise p_{en} en büyük asal sayıdır gerçeği ile çelişir. Sonuç olarak $\sim q$ yanlıştir, q doğrudur. $\square$

ör. q: $\sqrt{2}$ *irrasyoneldir* önermesini OEY ile kanıtlayalım.

$\sim q$: $\sqrt{2}$ *rasyoneldir* önermesini doğru kabul edelim. Şu halde, ortak bölenleri olmayan $a, b \neq 0$ tam sayılari vardır öyleki $\sqrt{2} = \frac{a}{b}$. Buradan $2 = \frac{a^2}{b^2}$ olur ki $a^2 = 2b^2$ bu a^2'nin cift olduğuna, dolayısıyla a'nin cift oldugu anlamina gelir.

a çift ise vardir $k \in \mathbb{Z}$ öyleki $a = 2k. a^2 = 4k^2$ olur. Buradan $4k^2 = 2b^2; b^2 = 2k^2$ çift, dolayisiyla b çift olur.

Buldugumuz a ve b nin cift olmasi durumu, a ve b nin ortak bölenleri olmamasi durumuyla çelişir. Sonuc olarak$\sim q$: $\sqrt{2}$ *rasyoneldir* önermesini doğru kabul ettigimizde bir çeliski bulduk. O zaman q doğru olur. $\square$

Varlıksal Önermelerin Kanitlanmasi

İcinde varliksal niteleyici ($\exists$) varsa, bu onermenin dogru oldugunu ispatlamak icin tek bir örnek icin onermenin dogru oldugunu ispatlamak yeterlidir.

(Evrensel olanda genel (generic) bir ornek uzerinden ispat yapiyorduk)

ör. İki asal sayinin toplami olarak iki farkli sekilde yazilan bir tam sayi vardir.

$(\exists\, z \in \mathbb{Z} : z = m + n \;\wedge\; z = k + l\, , \{m, n\} \neq \{k, l\} \subset P\,)$

Kanit: $10 \in \mathbb{Z}$ tamsayisi, $5 + 5$ ve $3 + 7$ seklinde iki asal sayinin toplami olarak iki farkli sekilde yazilabilir. Bu da önermeyi ispatlamak icin yeterlidir. $\square$

ör. r ve s iki tamsayı olsun. Şu halde $22r + 18s = 2k$ eşitligini sağlayan bir k tamsayısı vardır.

Kanit: $22r + 18s = 2k$ ise $11r + 9r = k$ dir. r ve s yi 1 alalım. Bu durumda $k = 20$ olur ve bir tamsayidir. $\square$

Evrensel Önermelerin Çürütülmesi

$\forall x \in S : P(x)$ gibi bir onermeyi çürütmek için S'nin $P(x)$ doğru olmadigi ($\sim P(x)$'in dogru oldugu) bir elamanini bulmamiz yeterlidir.

(Aslinda boyle yaparak $\forall x \in S : P(x)$ önermesinin tersi olan $\exists x \in S : \sim P(x)$ önermsini ispatlamis oluyoruz, boylece tersi dogru oldugundan $\forall x \in S : P(x)$ yanlış olur).

ör. Dünya kupasını kazanan her takım kuzey yarımküredendir.

Önermenin formal hali $\forall d \in D : kuzeyYarımküredendir(d)$ (D dünya kupasını kazanan takımlar kumesi). Fakat vardır $Brezilya \in D$ oyleki

$\sim kuzeyYarımküredendir(Brezilya)$. Tersi dogru oldugu icin onerme yanlistir.

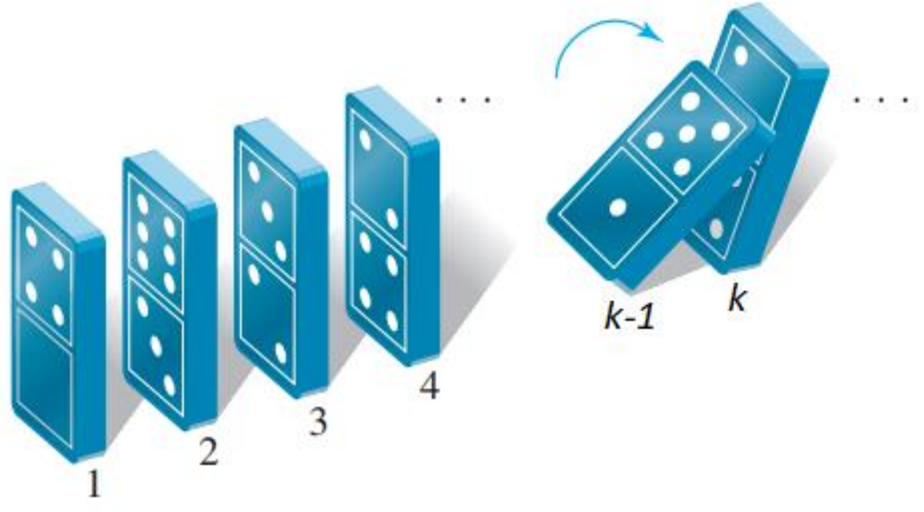
ör. $\forall a, b \in \mathbb{R}, a^2 = b^2 \Rightarrow a = b$

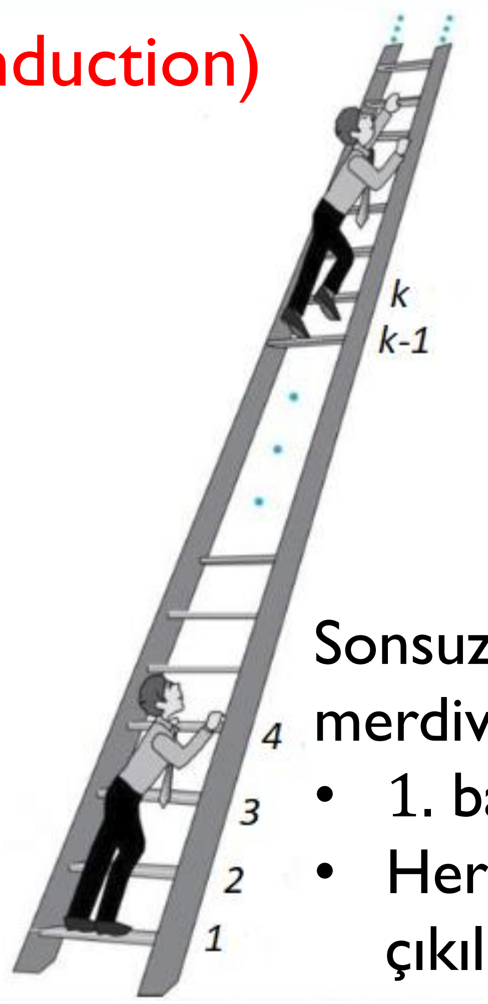
(Kareleri eşit olan reel sayilar biribirine eşittir).

$a = 1, \mathrm{b} = -1$ reel sayilarini alalim. Bu sayilarin kareleri birbirine eşittir: $a^2 = 1 = b^2$, fakat $a \neq b$.

(Not Hatirlarsak $p \Rightarrow q$ onermesi p dogru q yanlis oldugunda yanlisti. Ornekte $a^2 = b^2$aliyoruz yani p dogru; fakat $a \neq b$ buluyoruz yani q yanlış. Boyelce $p \Rightarrow q$ yanlış)

Matematiksel Tümevarım (Mathematical Induction)





* 1. domino düşer

* her ne zaman bir domino düşerse ondan bir sonraki domino da düşer.

Soru: k. domino da düşer mi?

$(k \geq 1)$

Sonsuz uzunlukta bir merdivenimiz var.

- 1. basamağa çıkılıyor
- Her ne zaman bir basamağa çıkılırsa bir sonraki basamağa da çıkılır.

Soru: k. merdivene de çıkılır mı?

$(k \geq 1)$

Matematikel tümevarım bir kanıt yöntemidir ve altta yatan mantık domino örneğindekine benzerdir.

0'dan yada herhangi bir pozitif tam sayıdan başlayarak tüm tamsayılar için geçerli onermeleri kanitlarken tümervarımla kanıt yapariz.

Tümevarımla Kanıt

$\forall\, n \in \mathbb{Z}^{\geq 0}: P(x)$ önermesinin tümevarımla kanitlarken aşağıdaki iki durumu kanitlariz:

1. temel durum (base case) $P(0)$
2. tümevarımsal durum (inductive case) her $n \geq 1, P(n-1) \Rightarrow P(n)$

ör. Negatif olmayan her tamsayi n ($\forall\, n \in \mathbb{Z}^{\geq 0}$) için: $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$

temel durum: $n = 0$ için $P(0)$ ispatlayalım. $\sum_{i=0}^{0} 2^i = 2^0 = 1.$

$n = 0$ için $2^{n+1} - 1 = 1$ olup eşitliğin sag ve sol tarafi birbirine esittir.

Tümevarimsal durum: $P(n-1)$ doğru olsun. Şu halde $\sum_{i=0}^{n-1} 2^i = 2^n - 1$.

Bu eşitligin her iki tarafina 2^n ekleyelim.

$2^n + \sum_{i=0}^{n-1} 2^i = 2^n - 1 + 2^n \Rightarrow \sum_{i=0}^{n} 2^i = 2 \cdot 2^n - 1 \Rightarrow \sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$

Boylece $P(n)$ doğru olur. $\square$

ör. $0 + 1 + \cdots + n = \frac{n(n+1)}{2}$ $(n \in \mathbb{Z}^{\geq 0})$ eşitliğini ispatlayalım.

Öncelikle bu eşitliği $\forall\, n \in \mathbb{Z}^{\geq 0}$ sahip oldugu bir ozellik olarak yazalim:

n'nin sahip oldugu P özelligi: $P(n)$: $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

temel durum: $n = 0$ için $0 = \frac{0(1)}{2} = 0$ olup $P(0)$ doğrudur.

tümevarımsal durum: $P(n-1)$ doğru olsun: $0 + 1 + \cdots + n - 1 = \frac{n-1(n)}{2}$

Eşitligin iki tarafina n ekleyelim: $0 + 1 + \cdots + n - 1 + n = \frac{n-1(n)}{2} + n = \frac{n^2-n+2n}{2} = \frac{n(n+1)}{2}$

Boylece $P(n)$ doğru olur. $\square$

Tümevarimsal durumu şu şekilde de kanitlayabiliriz.

$$\sum_{i=0}^{n} i = \sum_{i=0}^{n-1} i + n = \frac{n-1(n)}{2} + n = \frac{n(n+1)}{2}$$

$P(n)$ neden doğru olmak zorunda?

1. Temel durumdan dolayi $P(0)$'in doğru olduğunu biliyoruz. Tümevarimsal durumdan dolayi elimizde $n \geq 1, P(n-1) \Rightarrow P(n)$ var. $n = 1$ için $P(0) \Rightarrow P(1)$

$P(0)$ ve $P(0) \Rightarrow P(1)$ önermeleri doğru. Şu halde $P(1)$'de doğru (*Modus Ponens*'ten ötürü)

(Modus Ponens: $p \wedge (p \Rightarrow q) \Rightarrow q$)

2. $P(1)$ dogru. Tümevarimsal durumdan $P(1) \Rightarrow P(2)$ doğru. Modus Ponens'ten $P(2)$ doğru.
3. $P(2)$ dogru. Tümevarimsal durumdan $P(2) \Rightarrow P(3)$ doğru. Modus Ponens'ten $P(3)$ doğru.

....

Bu sırayla devam ederek ileride herhangi bir n için $P(n)$ doğru olur.

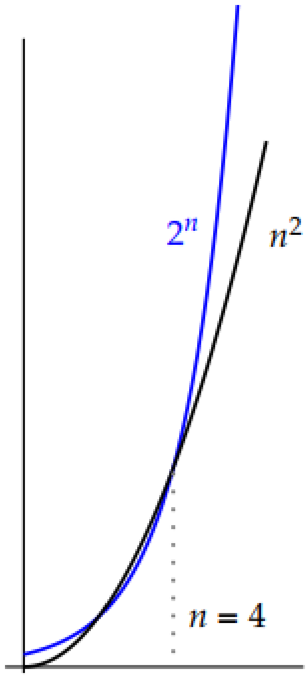
(n. domino taşı devrilir; n. basamağa çıkılır!)

Tümevarım ile Algoritmalari Kıyaslamak

Diyelimki bir problem icin iki algoritma gelistirdik. n elemanli bir S kumesi icin, birinci algoritma bu kumenin 2^n tane alt kümesini inceleyerek (tarayarak) bir cozum uretiyor; ikinci algoritma ise bu kumenin n^2 tane alt kumesini inceliyor. Bu iki algoritmadan genel olarak hangisi daha hizlidir?

İlk birkaç n değeri icin 2^n ve n^2 nin aldigi degerler:

n	2^n	n^2
0	1	0
1	2	1
2	4	4
3	8	9
4	16	16
5	32	25
6	64	36



$n \geq 4$ den sonra $2^n \geq n^2$

Görülüyor ki $n \geq 4$ den sonra $2^n \geq n^2$. Bunu tümevarımla ispatlayalim.

$n \geq 4$ için $P(n)$ özelligi $2^n \geq n^2$ olsun.

temel durum. $n = 4$ için $2^n = 16 = n^2$ olup özellik saglanir.

tümevarimsal durum. $P(n-1)$ doğru olsun. Bu durumda $2^{n-1} \geq (n-1)^2$ olur.

$P(n)$ nin dogru oldugunu gosterelim.

$$
\begin{aligned}
2^n = 2 \cdot 2^{n-1} &\geq 2 \cdot (n-1)^2 \\
&= 2n^2 - 4n + 2 \\
&= n^2 + (n^2 - 4n) + 2 \\
&\geq n^2 + 0 + 2 \\
&> n^2
\end{aligned}
$$

Böylece $2^n \geq n^2$ oldugu gösterilmis olur. Buna gore n^2 alt kümeyi inceleyen algoritma daha hizlidir diyebiliriz. $\square$

Not. Yukaridaki eşitsizlikte $n \geq 4$ oldugundan $n^2 \geq 4n$, yani $(n^2 - 4n) \geq 0$ bilgisini kullandik.

Tümevarım ile Algoritmanin Dogrulugunu Kanitlamak

Tümevarim ile bir algoritmanin dogrulugunu da kanitlayabiliriz.

ör. Şöyle bir rekürsif bir algoritmamiz olsun. Bu algoritma girilen bir sayının faktoriyelini bulur.

```
faktor(n):
1. if n=1 {
2.      return 1 }
3.   else
4. return n·faktor(n-1)
```

Tümevarımla bu algoritmanin faktoriyeli dogru hesapladigini kanitlayalim.

$P(n)$ özelligi `faktor(n)`$=n!$ (yani algoritmanin n icin faktoriyeli dogru hesaplamasi)

temel durum: $n = 1$ için `faktor(1)`$=1 = 1!$ (alg. 1.satirindan dolayi) $P(1)$ dogru.

tümevarımsal durum: $P(n-1)$ dogru olsun. Bu durumda `faktor(n-1)`$=(n-1)!$

`faktor(n)=n·faktor(n-1)` (alg.in 4.satirindan dolayi)

$$= n \cdot (n-1)! = n!$$

Su halde $P(n)$ dogru olur. □

Güçlü Tümevarım (Strong Induction)

Buraya kadar tümevarimla ispat yaparken $P(0)$ ve $P(n-1) \Rightarrow P(n)$ $(n \in \mathbb{Z}^{\geq 1})$ doğru olduklarini varsayarak ispat yaptik.

Fakat daha onceden de gordugumuz gibi $P(0)$ ve $P(n-1) \Rightarrow P(n)$ $(n \in \mathbb{Z}^{\geq 1})$ dogru oldugunu varsayarsak $P(0), P(1), P(2), P(3), \ldots, P(n-1)$ önermelerinin tamami dogru olur.

İşte güçlü tümevarimda $P(0), P(1), P(2), P(3), \ldots, P(n-1)$ önermelerinin ***tamamının*** doğru oldugunu varsayarak $P(n)$'nin dogru oldugunu göstereceğiz.

Güçlü Tümevarımla Kanıt

$\forall\, n \ \in \mathbb{Z}^{\geq 0}: P(x)$ önermesinin güçlü tümevarımla kanıtlarken aşağıdaki iki durumu kanitlariz:

1. temel durum (base case) $P(0)$
2. tümevarımsal durum (inductive case) her $n \geq 1, [P(0) \wedge P(1)^{\cdot} \wedge \cdots \wedge P(n-1)] \Rightarrow P(n)$

Not 1: Dikkat edin $[P(0) \wedge P(1)^{\cdot} \wedge \cdots \wedge P(n-1)]$ doğru kabul ediyoruz. Bunun dogru olabilmesi icin $P(0), P(1), \ldots, P(n-1)$ önermelerinin ***tamamı*** doğru olmak zorundadır.

Not 2 . Güçlü tümevarım aslında normal tümevarıma denktir: Güçlü tümevarımla kanıtlayabildigimiz her şeyi normal tümevarımla; normal tümevarimla kanıtlayabildigimiz her şeyi güçlü tümevarimla da kanıtlayabiliriz!

Not 3: Genel olarak güçlü tümevarımla kanit yapmak normal tümevarima göre daha kolaydir. Özellile tümevarımsal durumun kaniti güçlü tümevarimda daha kolaydir.

ör. Teorem: 1'den büyük her tamsayı bir asal sayıya bölünebilir.

Bu teoremi güçlü tümevarımla kanıtlayalım.

Bunun için öncelikle $\forall\, n \in \mathbb{Z}^{\geq 1}$ için $P(n)$ özelliğini tanimlayalim:

$P(n)$: n bir asal sayıya bölünebilir.

temel durum: $n = 2$ için; n, 2 asal sayısına bölünebilir. $P(2)$ doğrudur.

tümevarımsal durum: $n \geq 2$ için $P(2), P(3), \ldots, P(n-1)$ doğru olsun. Bu, $2,3, \ldots, (n-1)$ tamsayılarının bir asal sayiya bölünebildigi anlamina gelir.

$P(n)$ dogrulugunu kanitlamak icin 2 durumu göz önune alacagiz.

1. n asal ise n'nin bir asal boleni vardir, kendisidir.
2. n asal degilse n sayisini $n = a \cdot b$ $(a, b \in \mathbb{Z}^{\geq 1})$ seklinde yazabiliriz. Burada a ve b tamsayiıari 2 ile $(n-1)$ arasindadir. $(2 \leq a \leq n-1, 2 \leq b \leq n-1)$. Tumevarimsal hipotezden $P(a)$ ve $P(b)$ dogrudur. O halde a ve b nin asal bolenleri vardir. Bunlar p_1 ve p_2 olsun. $a = p_1 \cdot m$ ve $b = p_2 \cdot l$ $(m, l \in \mathbb{Z}^{\geq 1})$ seklinde yazabiliriz.

   $n = a \cdot b = p_1 \cdot m \cdot p_2 \cdot l$ olur ki n'nin p_1 ve p_2 gibi asal bolenleri olur. $P(n)$ dogru olur. □

ör. Teorem: Her positif tamsayi ikilik tabanda gosterilebilir.

Bu teoremi guclu tumevarimla ispatlayalim.

Öncelikle $\forall\, n \in \mathbb{Z}^{+}$ için $P(n)$ özelliğini tanimlayalim:

$P(n)$: n ikilik tabanda gosterilebilir.

n sayisini ikilik tabanda gosterebilmek $n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0$ seklinde yazabilmek demektir, cunku bu durumda $n = {c_r c_{r-1} \ldots c_2 c_1 c_0}_2$ olur.

Burada c_r 1 olmak zorundadir, diger $c_{r-1}, c_r c_{r-2}, \ldots, c_2, c_1, c_0$ 0 yada 1 olabilir.

temel durum: $n = 1$ icin $r = 0$ ve $c_0 = 1$ alirsak $1 = 1_2$ seklinde yazabiliriz. $P(1)$ dogru olur.

tumevarimsal durum: $P(1), \ldots, P(n-1)$ hepsi dogru olsun. Bu durumda n'den kucuk her pozitif tamsayi ikilik tabanda gosterilebilir.

n'nin teklik ciftlik durumuna gore $\mathrm{P}(n)$ nin dogrulugunu iki durumda ispatlayacagiz.

n ciftse: $n/2$ den kucuk bir tam sayidir. O halde ikilik tabanda yazilabilir:

$n/2 = c_r \cdot 2^r + \cdots + c_1 \cdot 2 + c_0 \; (c_r = 1, c_{r-1}, \ldots, c_1, c_0 \in \{0,1\})$

Esitligin her iki tarafini 2 ile carparsak

$n = c_r \cdot 2^{r+1} + \cdots + c_1 \cdot 2^2 + c_0 \cdot 2 \ (c_r = 1, c_{r-1}, \dots, c_1, c_0 \ \in \{0,1\})$

bu, n'nin ikilik tabanda yazilabilecegi anlamina gelir.

n tekse $n - 1$ cifttir, $(n-1)/2$ tamsayidir ve ikilik tabanda yazilabilir:

$(n-1)/2 = c_r \cdot 2^r + \cdots + c_1 \cdot 2 + c_0 \ (c_r = 1, c_{r-1}, \dots, c_1, c_0 \ \in \{0,1\})$

Her iki tarafi 2 ile carparsak:

$n - 1 = c_r \cdot 2^{r+1} + \cdots + c_1 \cdot 2^2 + c_0 \cdot 2 \ (c_r = 1, c_{r-1}, \dots, c_1, c_0 \ \in \{0,1\})$

$n = c_r \cdot 2^{r+1} + \cdots + c_1 \cdot 2^2 + c_0 \cdot 2 + 1 \ (c_r = 1, c_{r-1}, \dots, c_1, c_0 \ \in \{0,1\})$

bu, n'nin ikilik tabanda yazilabilecegi anlamina gelir.

Boylece iki durumda da n'nin ikilik tabanda yazilabilecegini gosterdik.

$\mathrm{P}(n)$ dogru olur.

$\square$