הרצאה 7:
משפט נקודת השבת
ומשפט האי-שלם של גודל
奶茶 米飲 qgمسفر SSD | C. דוג_started את הטפרה עד | D
משפט (למט הליכסון): תהי Γ יורה על שורגי של משפה של
(X substitutions 19 מהרצאות 6) נגנט הליגת היא B - ה- x מסתיימה בשפה של
נתן nosa Cavs G.ceil C ש- C. הקשתת החופשית חיידה B - הקדת קיימת nosa Cavs
לכל nosa Cavs
הנשמה A(x1,x2). נסמי את הנשמה
A(x1) עיניים. ∀x2(A(x1,x2) → B(x2))
∀x2(A(m,x2)   . קיימת nosa Cavs שפולה היא C. הכלום היא φ(m) . φ(φ(x1)) → B(x2))
יהי מיספר גודל של q שפולה: nosa Cavs
Γ | A(m,q) , Γ - D מיספר גודל של nosa Cavs A.موسפ ש- Miyanega את D(m) = q, D
קודם נוכיח כי \( C, \Gamma \vdash B(\Box C) \):

1. \( \forall x_2(A(m,x_2) \rightarrow B(x_2)) \)
   \( \text{(ננמ) } C \)
2. \( A(m,q) \rightarrow B(q) \)
   \( \text{A4, MP, 1} \quad D \)
3. \( A(m,q) \)
   \( \text{כзи מנייצת את } A \text{ כジー מנייצת את } A \)
4. \( B(q) \text{ "=} B(\Box C)" } \)
   \( \text{MP, 2, 3} \)

.: \( \Gamma \vdash C \rightarrow B(\Box C) \) : עיון משבט הדדוקציה.
נוכיח כי $B[ C ]$, $A(\overline{m},x_2), \Gamma \models B(x_2)$

1. $B(\overline{q})$
2. $A(\overline{m},x_2)$
3. $\exists! x_2 A(\overline{m},x_2)$  
  못וות של $D$ משם ש-$D$ מייצגת את $A$
4. $A(\overline{m},\overline{q})$
5. $x_2 = \overline{q}$
6. $B(x_2)$

$B(\overline{C}), \Gamma \models A(\overline{m},x_2) \rightarrow B(x_2)$

על ידי ד"ד הפסגיטציה:

. $B(\overline{C}), \Gamma \models \forall x_2(A(\overline{m},x_2) \rightarrow B(x_2))$ "$= C$" ,GEN

. $\Gamma \models B(\overline{C}) \rightarrow C$

נשמוח במשפט הפסגיטציה עוד פעמים נקבה

מ"ש.ל.
ההגדרה: נניח \( \Gamma \) היא תורה מעל שפה של \( \text{FA} \). \( \Gamma \) \( \vdash \exists x \phi(x) \) אם ו Только אם \( \forall n \in \mathbb{N}, \Gamma \vdash \neg \phi(n) \).すべの場合 \( \Gamma \) \( \vdash \exists x \phi(x) \).

הענפה: \( \exists x \phi(x) \) \( \vdash \exists x \phi(x) \).}

הוכחה: \( \phi(x) \) \( \vdash \exists x \phi(x) \) \( \forall n \in \mathbb{N}, \phi(n) \wedge \neg \phi(n) \). לכל \( n \), \( \exists x \phi(x) \). מ.ש.ל.
משפט איני-שלמות של גודל

המי המורה על השפת של FA. אנו נניח כי \( \Gamma \) מקיימת את התכונות הבאות:

1. היחס \( PrAx(x) \) הוא רקורסיבי.
2. \( \Gamma \vdash 0 \neq 1 \)
3. כל פונקציות רקורסיביות נמצאות בלשון \( \Gamma \).

משפט האי-שלמות של גודל

נניח כי היחס \( Pf \) ניתן לביטוי על ידי \( Pr(x_1,x_2) \) ונסמן את \( \forall y \sim Pr(y,x) \) על ידי \( B(x) \).

נניח כי היחס \( Pf \) נימקי לביטוי על ידי \( Pr(x_1,x_2) \) ונסמן את \( \forall y \sim Pr(y,[ C ]) \) על פי מושג נקודת השבת קיימ פסוק \( C \) כי- ש-
משפט (משפט אי-שלמות של גודל):

合作共赢, אם \( \Gamma \vdash C \) אז \( \Gamma \vdash \sim C \) ו-合作共赢, אם \( \Gamma \vdash \sim C \) אז \( \Gamma \vdash C \).

הוכחה:

\( Pf(r,q) \) נגזר בשילוב עם \( \sim C \) ו-合作协议 \( r \), ו-合作协议 \( \Gamma \vdash C \) \( \Gamma \vdash Pr(r,\lceil C \rceil) \) \( \Gamma \vdash Pr(r,q) \). לכל \( C \) ההypotheses \( \Gamma \vdash \sim Pr(r,\lceil C \rceil) \) \( \Gamma \vdash \forall y \sim Pr(y,\lceil C \rceil) \). זה סותר את ההנחה ש-合作协议 \( \sim \). זה סותר את ההנחה \( \sim \).

合作协议, אם \( \Gamma \vdash \sim C \)在线咨询 \( \sim C \)合作协议, נובע מהתקף \( \Gamma \vdash \exists y Pr(y,\lceil C \rceil) \) \( \sim C \)在线咨询 \( \Gamma \vdash Pf(n,q) \)在线咨询 \( n \)在线咨询 \( \exists y Pr(y,\lceil C \rceil) \)在线咨询 \( \sim C \).在线咨询 \( \Gamma \vdash Pf(n,q) \)在线咨询 \( n \)在线咨询 \( \exists y Pr(y,\lceil C \rceil) \)在线咨询 \( \sim C \).在线咨询 \( \Gamma \vdash Pf(n,q) \)在线咨询 \( n \)在线咨询 \( \exists y Pr(y,\lceil C \rceil) \)在线咨询 \( \sim C \).在线咨询 \( \Gamma \vdash Pf(n,q) \)在线咨询 \( n \)在线咨询

מ.ש.ל.
הגדולה: קבוצת מספרים طبيعيים נקראת רקורסיבית אם היא זו המורידה \[ \{ n \mid R(n) \} \]
כפולה הוא множество רקורסיבי. נסמן \( T \) את הקבוצה של מספרי \( R \).

נוכל לכל המשפטים של \( FA \).

משפט: אם \( T \)_square

הוכחה: נניח בשילוב עם \( T \) רקורסיבית, ווהי \( T \) נסחה המבנית את \( q \). \( \forall \) \( q \in \mathbb{N} \)

עיט להמח הלכוס קיימ פסוק \( T \) המקיים: \( U \).

נוכל \( U \).

\( U \) \( \leq \) \( Tm(\overline{U}) \).

יפלו \( U \) \( \rightarrow \) \( Tm(q) \) \( \leq \) \( U \) \( \rightarrow \) \( q \in \mathbb{T} \).

לכן \( T \) \( \leq \) \( Tm(q) \).

לפ.ל.
הנה הדרכה: אם נcidade פסוק $A$ לא נחת בלכמה - או אם $A$ - $\Gamma \vdash A$.
מסקנה: אם $\Gamma$ -$\omega$ -eğiבי ואז קרימת הנוסחה שלא נחת בלכמה - $\Gamma$.

משפט: אם $A$عزيבי, ואז קרימת הנוסחה $Tr(x)$ כל שערור פסוק $A$. $\vdash A \equiv Tr([A])$.

הוכחה: ניקח קרימי $C$ הנקרא $\vdash C \equiv \sim Tr([C])$.

מהניחה נובע כי: $\vdash C \equiv Tr([C])$.

כלומר: $\vdash Tr([C]) \equiv \sim Tr([C])$.

מ.ש.ל.
האריתמטייקה של פרסבוגר
האקסיומות של \( P \):

\[
\begin{align*}
\text{S1} & : & x \not\equiv y & \rightarrow (x \not\equiv z \rightarrow y \not\equiv z) \\
\text{S2} & : & x \not\equiv y & \rightarrow x' \not\equiv y' \\
\text{S3} & : & 0 \neq x' \\
\text{S4} & : & x' \not\equiv y' & \rightarrow x \not\equiv y \\
\text{S5} & : & x + 0 \not\equiv x \\
\text{S6} & : & x + y' \not\equiv (x+y)' \\
\text{S9} & : & A(0) \rightarrow (\forall x(A(x) \rightarrow A(x'))) \rightarrow \forall x A(x)), \ A \ \text{עבור כל נוסחה}
\end{align*}
\]

\( S7 \) \( x \cdot 0 \not\equiv 0 \)

\( S8 \) \( xy' \not\equiv xy + x \)
 mañana \( x < y \) \( \exists z (x + z' = y) \)

 mañana \( x \equiv y \ (mod \ n) \) \( \exists z (x = y + nz) \lor y = x + nz \)

 קיצורים

 משפט: שלמה וניתנת להכרעה.

 \( t < r \) לכל נסחא של \( P \) שקולה לנוסחה שמתכונתilit מנוסחאות וחקירות מזירות

 או

 \( t \equiv r \ (mod \ n) \) אם ומקסם החשש \( t \neq r \) המashtra מתאם מיתרי� מזירה מזירות

 why (מדוע?)}.
הוכחת הלמה: מספיק להראות שלכל נססה של הצורה \( \exists x \varphi(x) \), כאשר \( \varphi (x) \) היא צירוף פסוקי של נסחות אטומיות ונוסחאות \( t < r \) או \( t \equiv r \pmod{n} \) שעוקב היא נססה שמתכונבת מנוסחאות \( t < r \) או \( t \equiv r \pmod{n} \) באמצע התשימים \( \land \). כלומר, ההוכחה היא יニアידוקייה על "העמק הכמות" של הנוסחה.

ובכן, התיה \( \varphi (x) \) צירוף פסוקי של נסחות אטומיות ונוסחאות \( t < r \) או \( t \equiv r \pmod{n} \). בסיטואציה זו, \( t < r \) או \( t \equiv r \pmod{n} \), בנחלות בשתי דוגמאות נתקל את כל השלילות לנוסחות אשר מתאימות נובעת ב- \( \varphi(x) \) את ההחלפות השקולות הבאות:

\( (t < r') \land (r < t') \) - \( t = r \)
\( (t < r) \lor (r < t) \) - \( t \neq r \)
\( r < t' \) - \( \sim (t < r) \)
\( \sim (t \equiv r \pmod{n}) \)
\( t \equiv r + 1 \pmod{n} \lor \ldots \lor t \equiv r + n - 1 \pmod{n} \)

לכל מותר לנוית \( \sim \) \( \varphi(x) \) צירוף פסוקי של נסחתות \( t < r \) או \( t \equiv r \pmod{n} \)
ע"י פעולות אריתמטיות נぶり את \( t \equiv r \pmod{n} \) לצורה \( t \equiv r_{1} \pmod{n} \)

- טור \( r_{1} \) ו- \( r_{2} \) לא מכילים את \( x \).

- נסחיר את הקטן מהגדול והPrivateKey \( mx + t_{2} \equiv r_{2} \pmod{n} \)

- \( mx \equiv r_{3} \pmod{n} \) \( (n - 1)t_{2} \) והPrivateKey \( x \).

- \( kx + t_{1} \equiv lx + r_{1} \pmod{n} \)

- \( mx + t_{2} \equiv r_{2} \pmod{n} \)

- \( kx \) \( \equiv \) \( l \cdot x \) \( \equiv \) \( r_{1} \pmod{n} \)

- \( mx + t_{2} \equiv r_{2} \pmod{n} \)

- \( mx \equiv r_{3} \pmod{n} \) \( (n - 1)t_{2} \) והPrivateKey \( x \).

- \( x \equiv q_{1} \pmod{n} \) \( \bigvee \ldots \bigvee \) \( x \equiv q_{j} \pmod{n} \)

- \( mx \equiv i \pmod{n} \) \( i=0,1,\ldots,n-1 \) \( ,mx \equiv i \pmod{n} \)

- \( \bigvee_{i=0}^{n-1} r_{3} \equiv i \pmod{n} \) \( \wedge mx \equiv i \pmod{n} \) \( -b \)

- \( bx \equiv i \pmod{n} \) \( i=0,1,\ldots,n-1 \) \( \wedge mx \equiv i \pmod{n} \)

- \( (\psi_{i})_{ij}(x) \wedge \phi_{i}(x) \) \( x \equiv q_{1} \pmod{n} \) \( \bigvee \ldots \bigvee x \equiv q_{j} \pmod{n} \)

- \( mx \equiv i \pmod{n} \)

- \( t \equiv r \pmod{n} \) \( \wedge mx \equiv i \pmod{n} \)

- \( t \equiv r \pmod{n} \) \( kx + t < r \) \( \wedge kx + t < r \)

- \( t \equiv r \pmod{n} \) \( kx + t < r \) \( \wedge mx \equiv i \pmod{n} \)

- \( t \equiv r \pmod{n} \) \( kx + t < r \) \( \wedge mx \equiv i \pmod{n} \)

- \( t \equiv r \pmod{n} \) \( kx + t < r \) \( \wedge mx \equiv i \pmod{n} \)
נוסף השכרות בשכבות.

 vess

 questão ב, אינה שקר

(\mod n)

עבור

, \quad q < n

, \quad n - q

עובר ו- q

x \equiv q \pmod{n}

איננה שקר,ازي מוטר להחליפילוות ב-

מתאימים (איך נובע?).

מתشهاد השאריות הסיני נובע שאם הקוניגונקציה

\begin{align*}
  x & \equiv q_1 \pmod{n_1} \land \cdots \land x \equiv q_j \pmod{n_j} \\
  \text{כאשר} \quad & q < n \end{align*}

, \quad i = 1,2,\ldots,l , kx + t < r_i

, \quad \forall i = 1,2,\ldots,l , kx + t < r_i

נדרג את הקוניגונקציה \( \exists x \land \phi_j(x) \). ונשים את הקוניגונקציה \( \phi_j(x) \) ואת \( \exists x \land \phi_j(x) \) השיוויון המשולב של \( q \) - השיוויון \( q \) שמעניינו ב-

\( x \equiv q \pmod{n} \) (איך נובע?).

לשים את הקוניגונקציה \( \exists x \land \phi_j(x) \) השיוויון המשולב של \( q \) - השיוויון \( q \) שמעניינו ב-

meaning- 

\( P \models \exists x \phi(x) \equiv \bigvee_i (\exists x \land \phi_{ij}(x) \land \psi_i ) \)

, \quad \forall i = 1,2,\ldots,l , kx + t < r_i

, \quad \forall C_i \quad P \models \land_{i=1}^l kx + t < r_i \equiv \bigvee_{i=1}^l C_i \land \bar{C_i}

"ככ讀取ה" שחיי בסל היחידה \( kx + t < r \) קורגוואנדצה את זה וא-شبهויהם בין האורורה

. הר

. \quad r < kx + t

נסעה אתו דבר עם א-شبهויהם בין האורורה
catezah נבצל קוניגונקציה של בשכל הitaire קוניגונקציה אחת, או-şıיוויוןくん הירפה $r < kx + t$ ואת ו-šיוויוןくん ההערה $kx + t < r$.

המקרה הביאים של קוניגונקציה.

•להונות קניונים זהים לקניון

$\exists x(kx + t < r_1 \land r_2 < kx + t)$

. $P \Rightarrow \exists x(kx + t < r_1 \land r_2 < kx + t) \equiv r_2 < r_1 \land t < r_1$

אם $1$, אז $k = 1$

אם $1$, נresher את $k > 1$.

ב- $kx + t < r_1 \land r_2 < kx + t$.

"$x \equiv 0 \pmod{k}$ " $\land x + t < r_1 \land r_2 < x + t$

למקרה המתיימר הביאים.

•להונות קוניגונקציה של קניונים

$\exists x(x \equiv q \pmod{n} \land r_2 < kx + t)$

$\exists x(x \equiv q \pmod{n} \land kx + t < r_2)$

(או-şıיוויון השני tras).
המקרה העיקור: הקונינקציה היא מהצורה:

\[ x \equiv q \ (\text{mod } n) \land kx + t < r_1 \land r_2 < kx + t \]

הנстроитель

\[ \exists x (x \equiv q \ (\text{mod } n) \land kx + t < r_1 \land r_2 < kx + t) \]

שקולו Lah

שקולו ל-

\[ \exists x (x \equiv qk \ (\text{mod } nk) \land x + t < r_1 \land r_2 < x + t) \]

נолית את הנוסחה האחראית ב-

\[ (r < t \land t + m < s) \lor (t < r' \land \bigvee_{i=1}^{l} (r + i < s \land r + i \equiv m + t \ (\text{mod } l))) \]

מסקנה: פונקציות הcekal לא נוגעת להפצצה ב-

\[ P \models \phi \]

מסקנה: היחס הורחב משמרת של \( P \) לא לכל נוסחה \( \phi \) של \( P \)

\[ P \models \phi \]