לוגיקה באימות פורמלי

הדר פרנקל

המחלקה למדעי המחשב, אוניברסיטת בר אילן

אימות פורמלי?

פיתוח שיטות מתמטיות להוכחת נכונות
של תכניות מחשב

לוגיקה...??

כל החתולים המעופפים סגולים

דנה רוצה לאמץ חיה סגולה **או** ירוקה, **וגם לא** מעופפת

כל התנינים מעופפים

הבעת שפה טבעית
באופן מתמטי

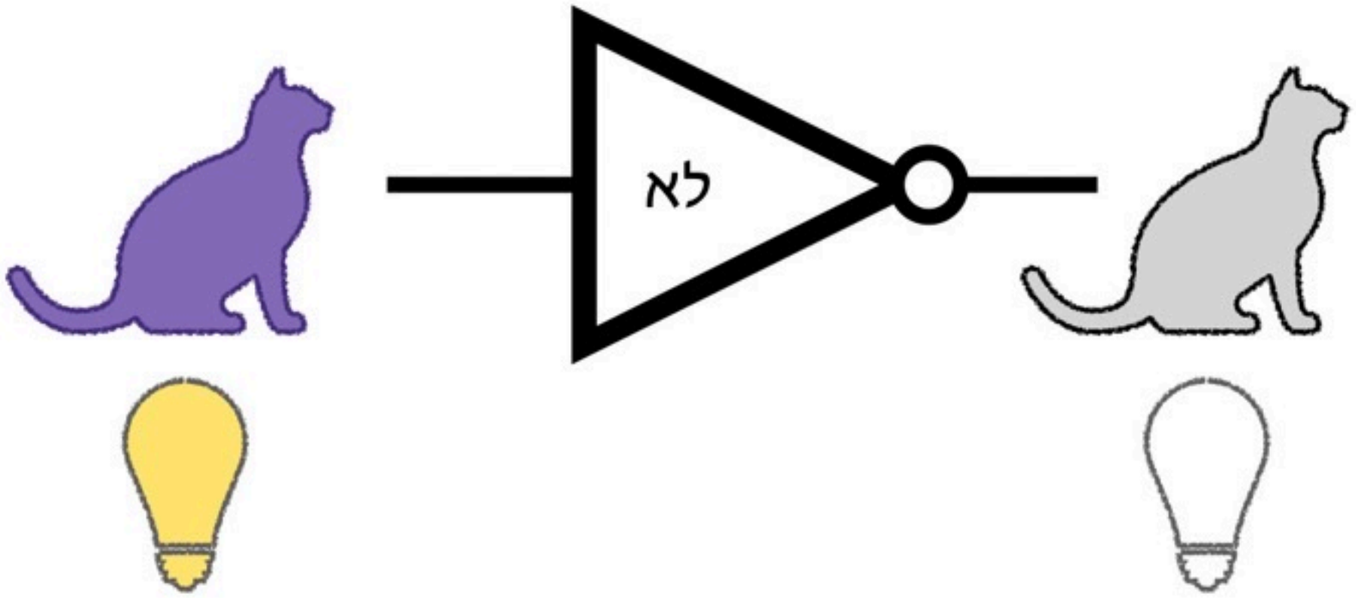
(1) דנה יכולה לאמץ חתול **ולא** תנין

(2) דנה יכולה לאמץ תנין **או** חתול

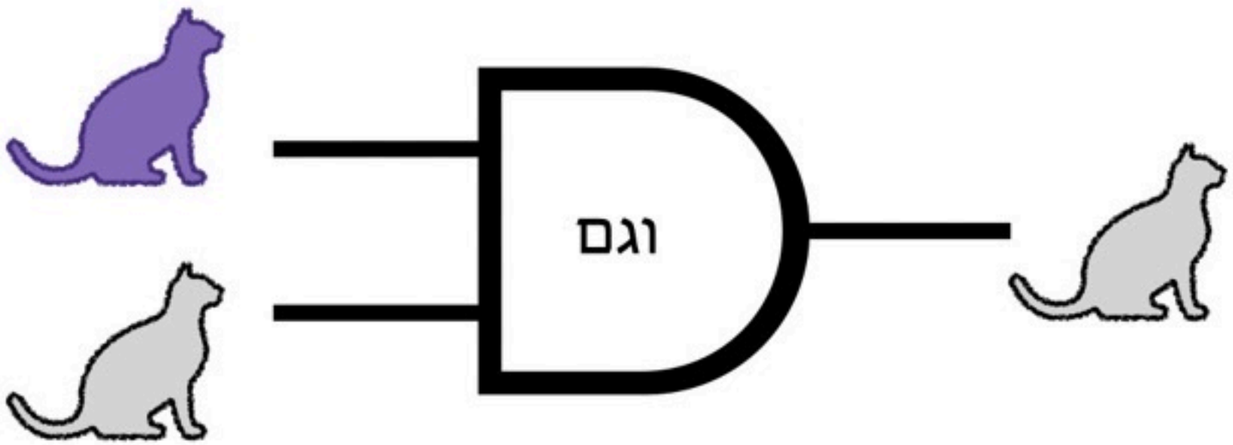
(3) דנה יכולה לאמץ חתול **ו**תנין

(4) דנה יכולה לאמץ ציפור

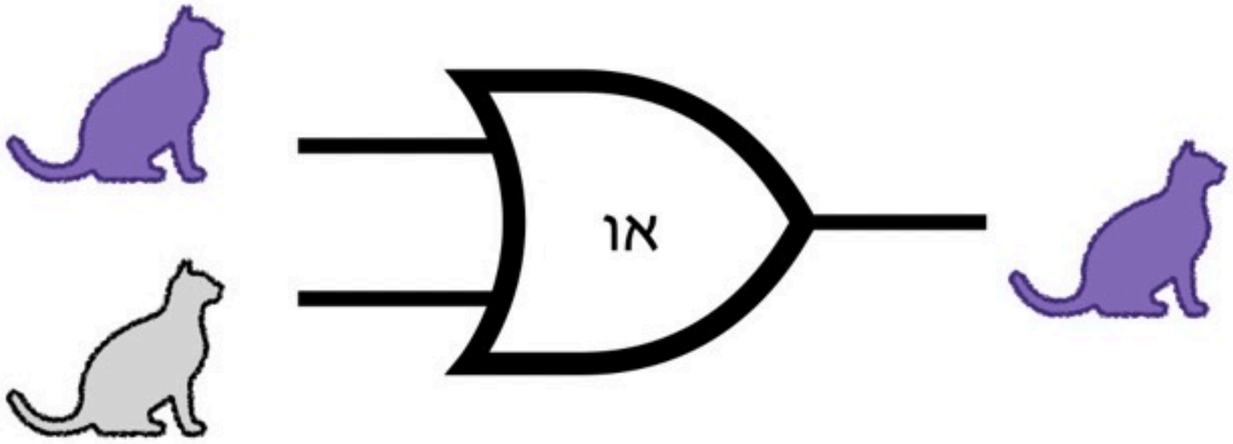
מה בין חתולים סגולים למחשבים?



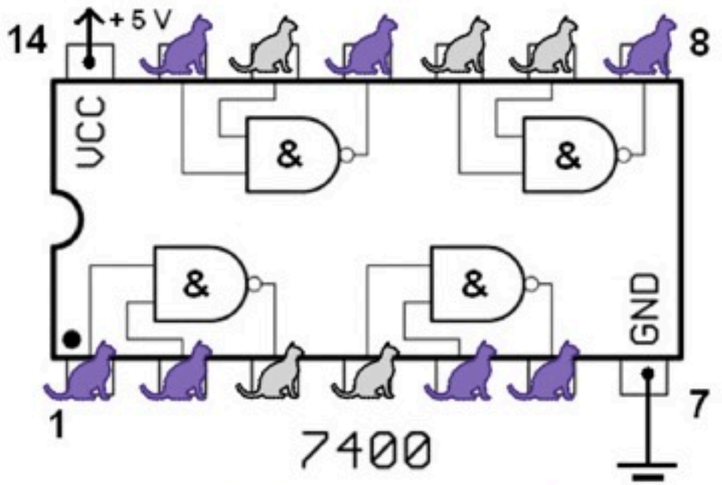
מה בין חתולים סגולים למחשבים?

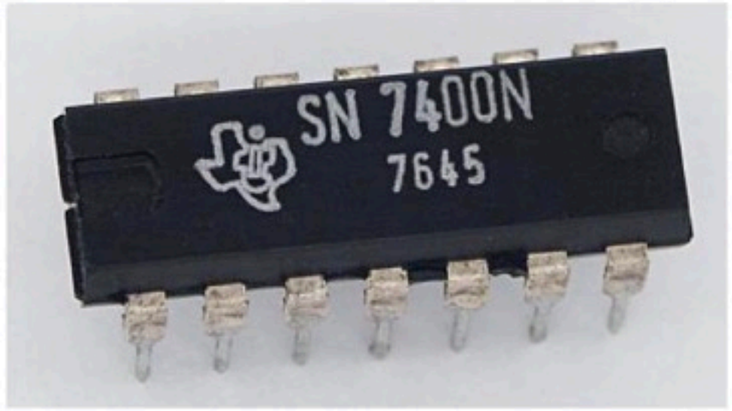


מה בין חתולים סגולים למחשבים?



מה בין חתולים סגולים למחשבים?



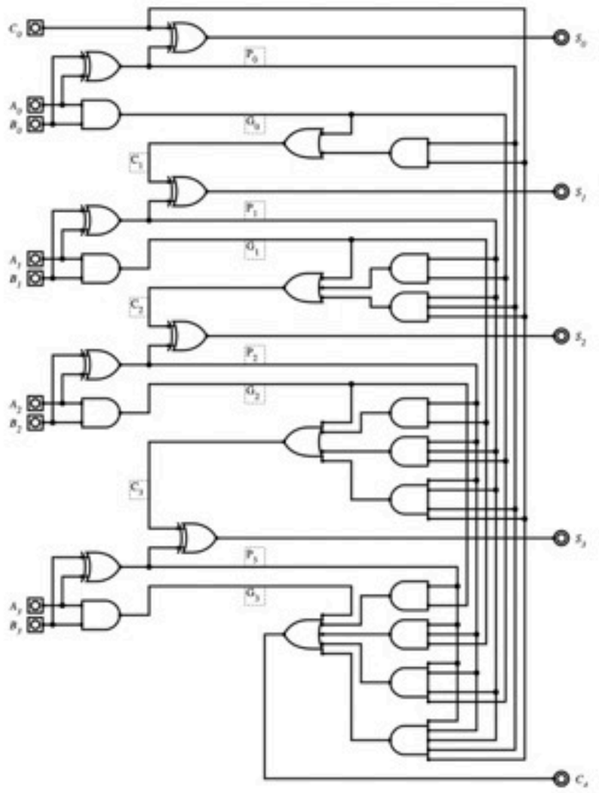


מה עושים עם זה?

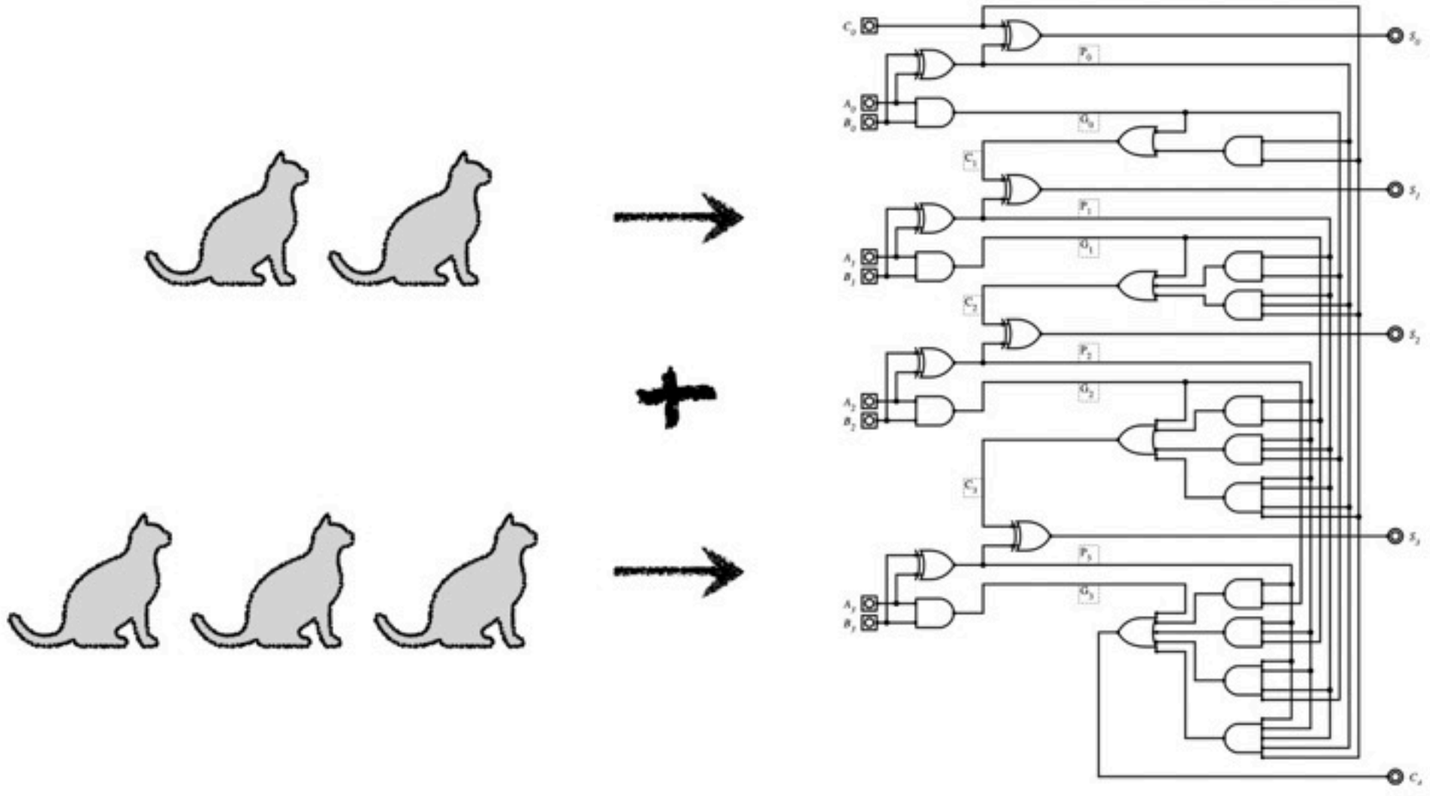
עוד

מה עושים עם זה?

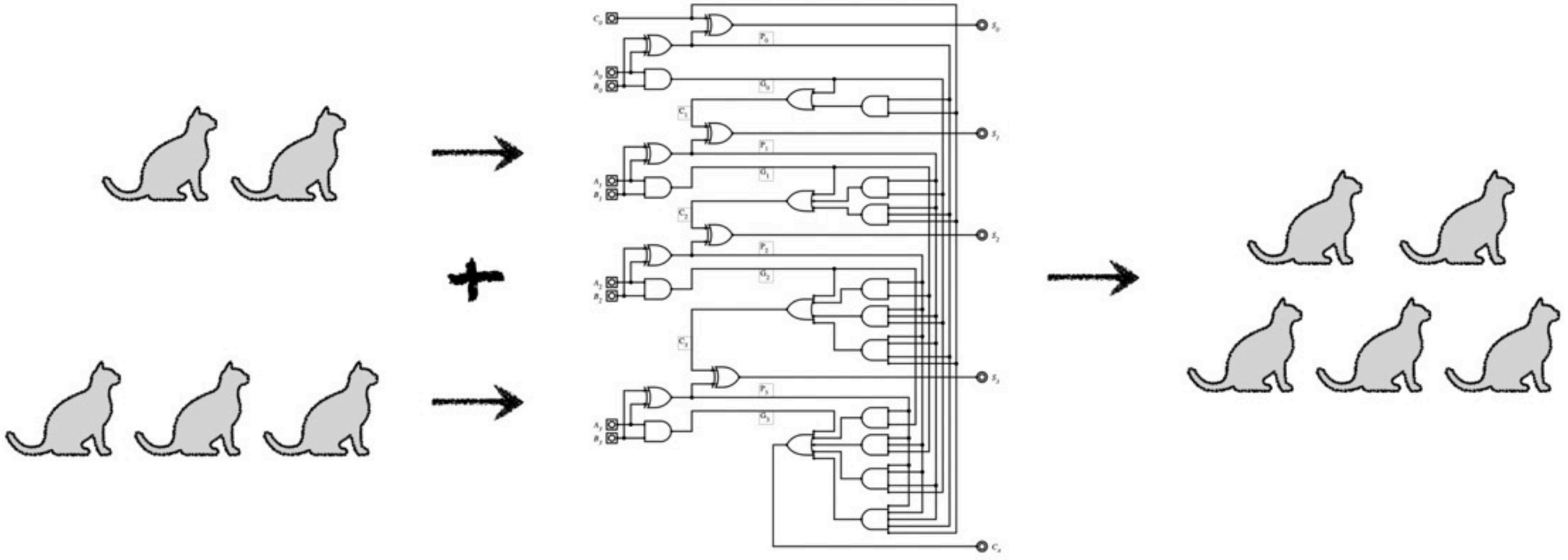
האם תכנית המחשב נכונה?



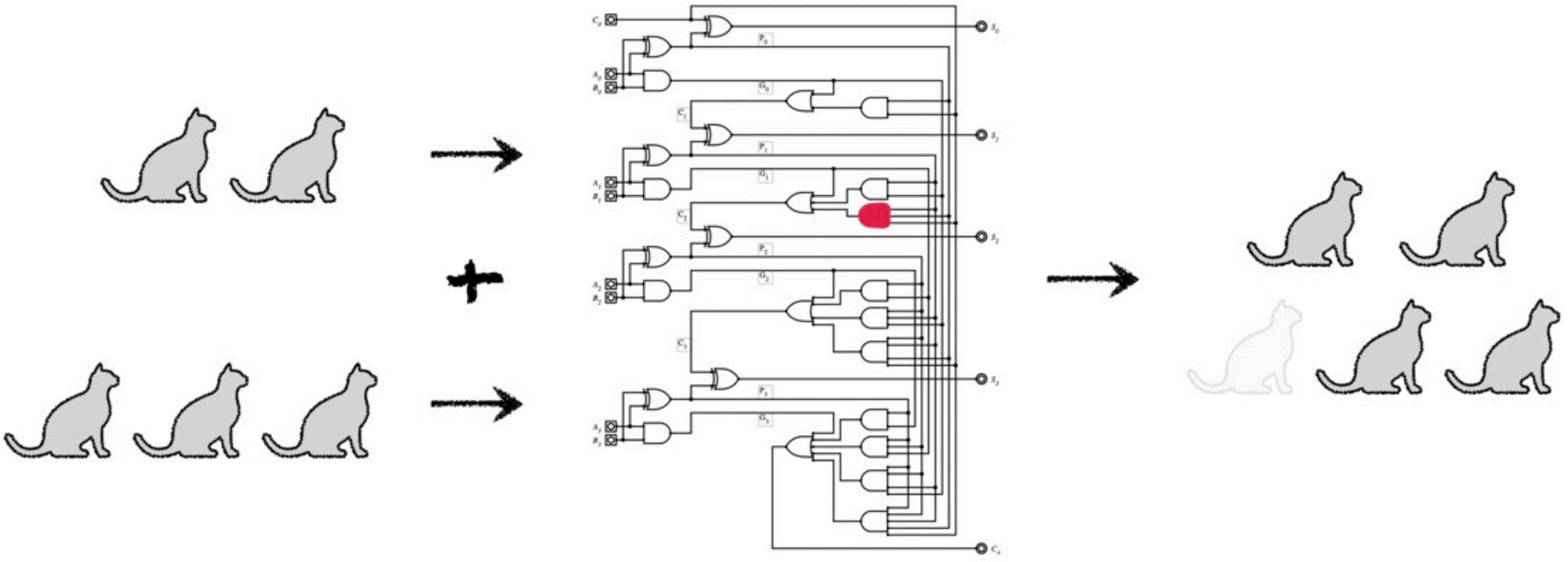
האם תכנית המחשב נכונה?



האם תכנית המחשב נכונה?



האם תכנית המחשב נכונה?

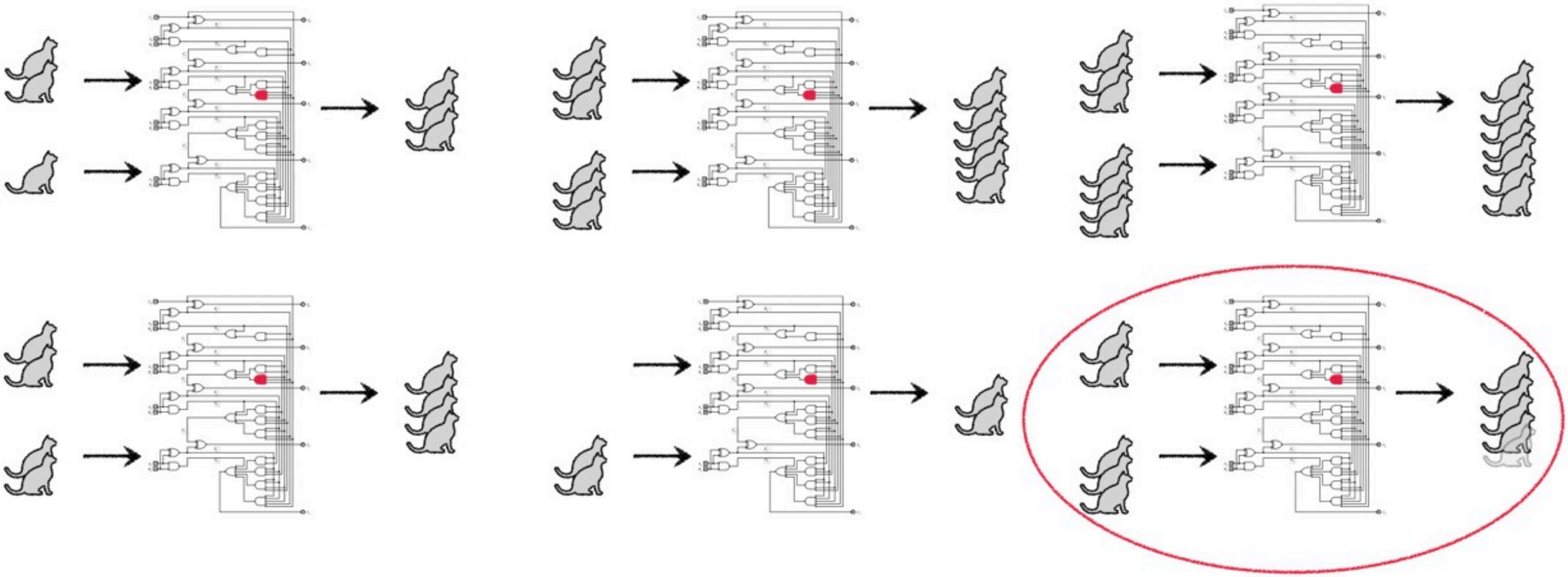


האם תכנית המחשב נכונה?

חיפוש באגים QA

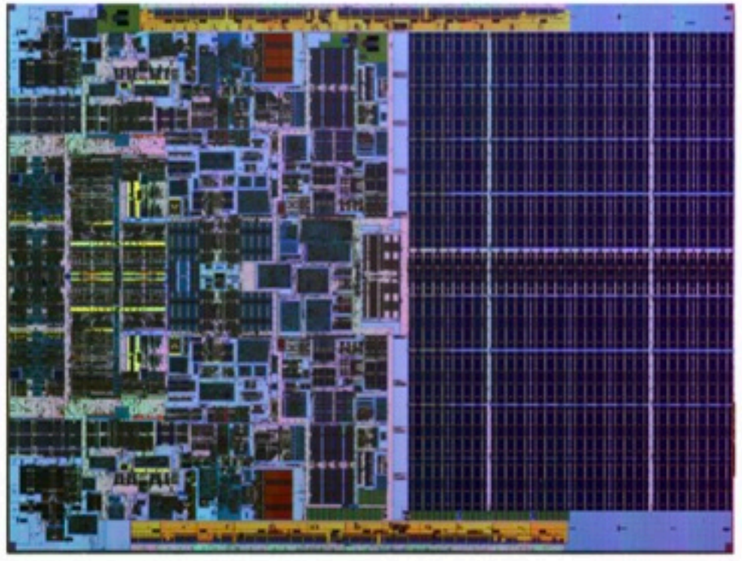
האם תכנית המחשב נכונה?

חיפוש באגים QA



תכניות גדולות...

מערכות חיוניות
טעויות יכולות להיות
קריטיות!



מעבד CPU

תא בקרה של מטוס

מכשור רפואי

כשלונות גדולים :(

1994: באג במעבדי פנטיום

Recall שעלה לאינטל כחצי מיליארד דולר

כשלונות גדולים :(

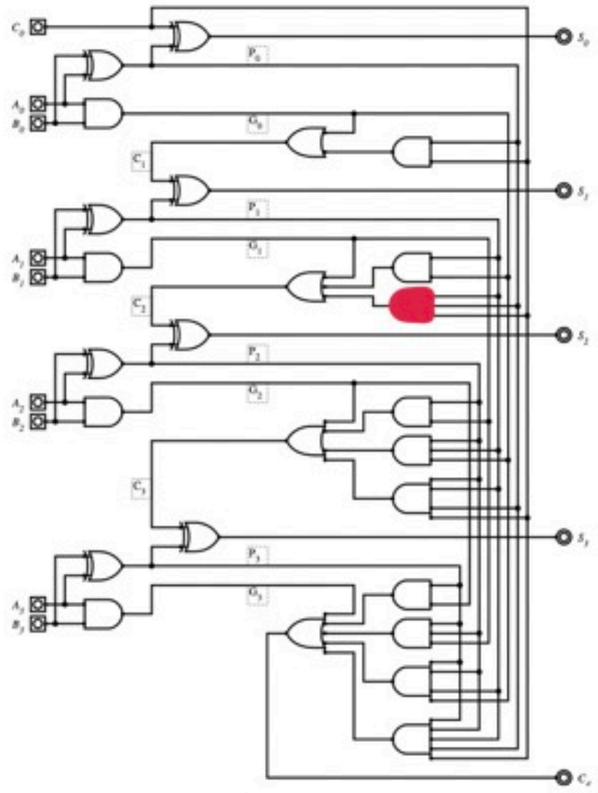
1994: באג במעבדי פנטיום

Recall שעלה לאינטל כחצי מיליארד דולר

1996: באג בתוכנת ההנחיה של משגר הלוויינים אריאן 5

הפעלת את מנגנון ההשמדה העצמי

הוכחה שהתכנית נכונה



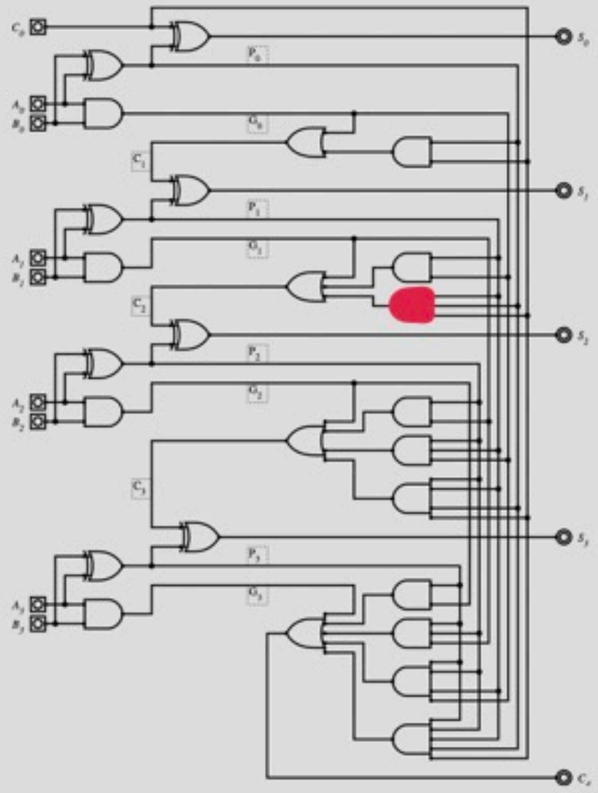
מפרט:
מה התכנית
אמורה לעשות

הוכחה שהתכנית נכונה

אימות פורמלי

האם התכנית
מספקת את המפרט?

מפרט:
מה התכנית
אמורה לעשות



מפרטים

שובה של הלוגיקה!

לוגיקה...??

כל החתולים המעופפים סגולים

דנה רוצה לאמץ חיה סגולה **או** ירוקה, **וגם לא** מעופפת

כל התנינים מעופפים

הבעת שפה טבעית
באופן מתמטי

(1) דנה יכולה לאמץ חתול **ולא** תנין

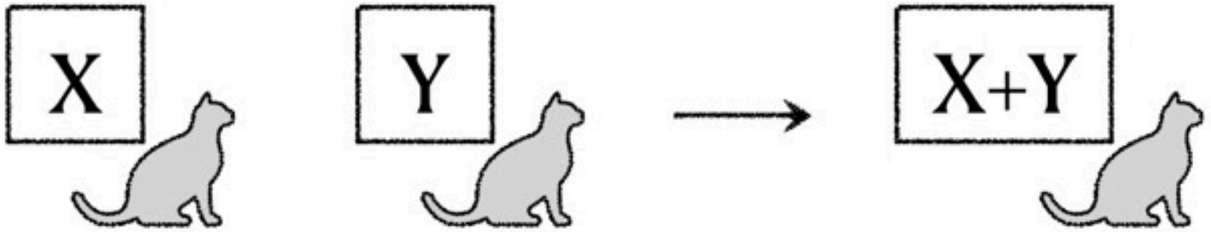
(2) דנה יכולה לאמץ תנין **או** חתול

(3) דנה יכולה לאמץ חתול **ו**תנין

(4) דנה יכולה לאמץ ציפור

מה התכנית
אמורה
לעשות

מפרטים



$$\forall x, \forall y \,.\, f(x, y) = x + y$$

מה התכנית אמורה לעשות

מפרטים

התנהגות של תכניות לאורך זמן

כל פעם שחתול אפור וסגול נפגשים, הם מיילים

$$\Box(\text{gray-cat} \wedge \text{purple-cat} \rightarrow \text{meow})$$

מפרטים

התנהגות של תכניות לאורך זמן

מה התכנית אמורה לעשות

כל פעם שיש אור ירוק ברמזור אחד, יש אור אדום בשני

$$\square(\text{green \#1} \leftrightarrow \text{red\#2})$$

מה התכנית אמורה לעשות

מפרטים

התנהגות של תכניות לאורך זמן

כל פעם שיש אור ירוק ברמזור אחד, יש אור אדום בשני

$$\square(\text{green \#1} \leftrightarrow \text{red\#2})$$

תמיד, בסופו של דבר האור יתחלף לירוק

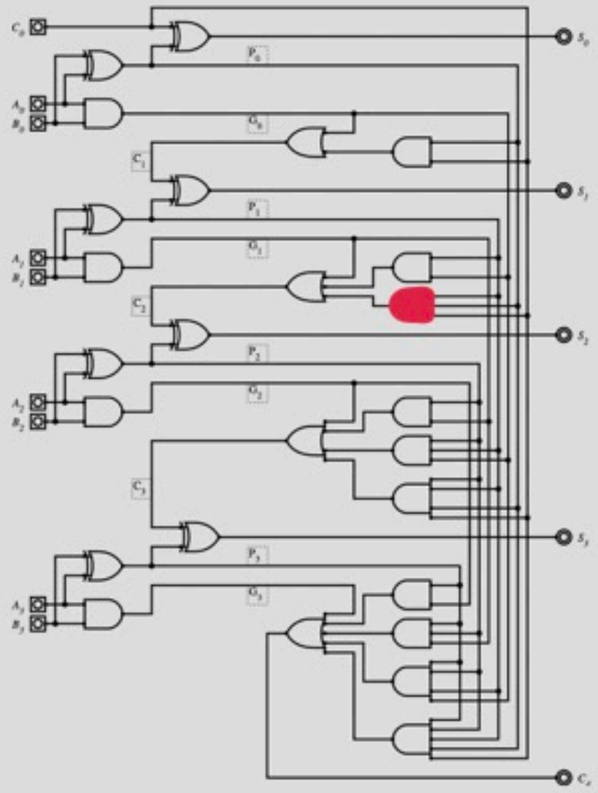
$$\square\Diamond\text{green}$$

הוכחה שהתכנית נכונה

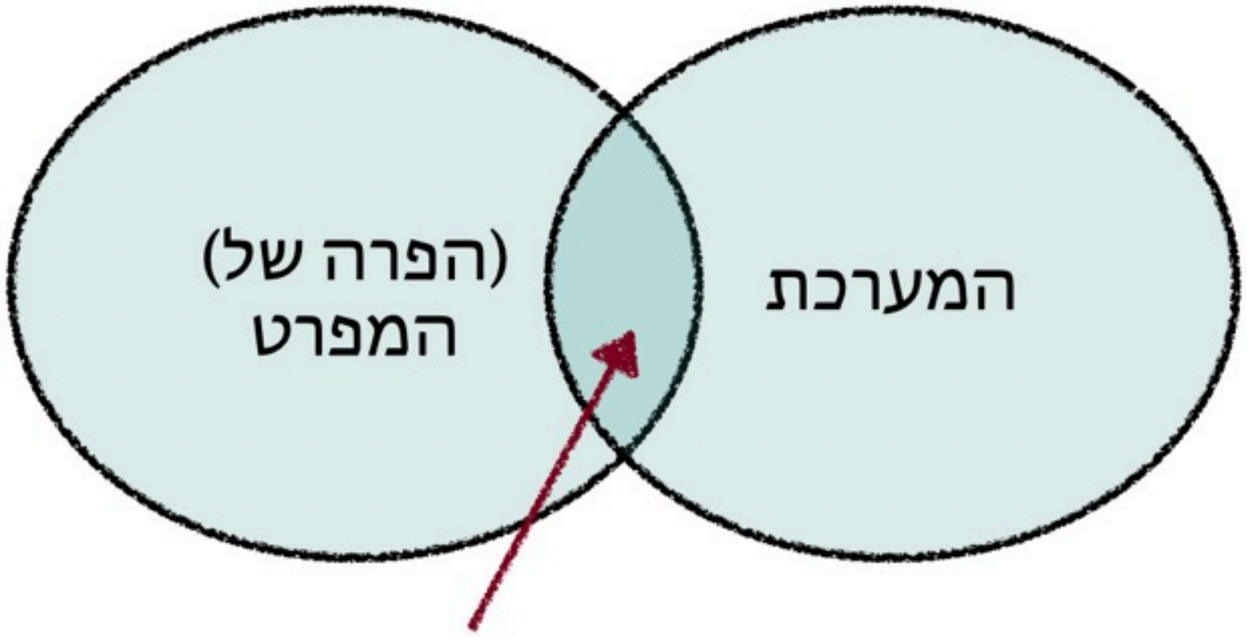
אימות פורמלי

האם התכנית
מספקת את המפרט?

מפרט:
מה התכנית
אמורה לעשות

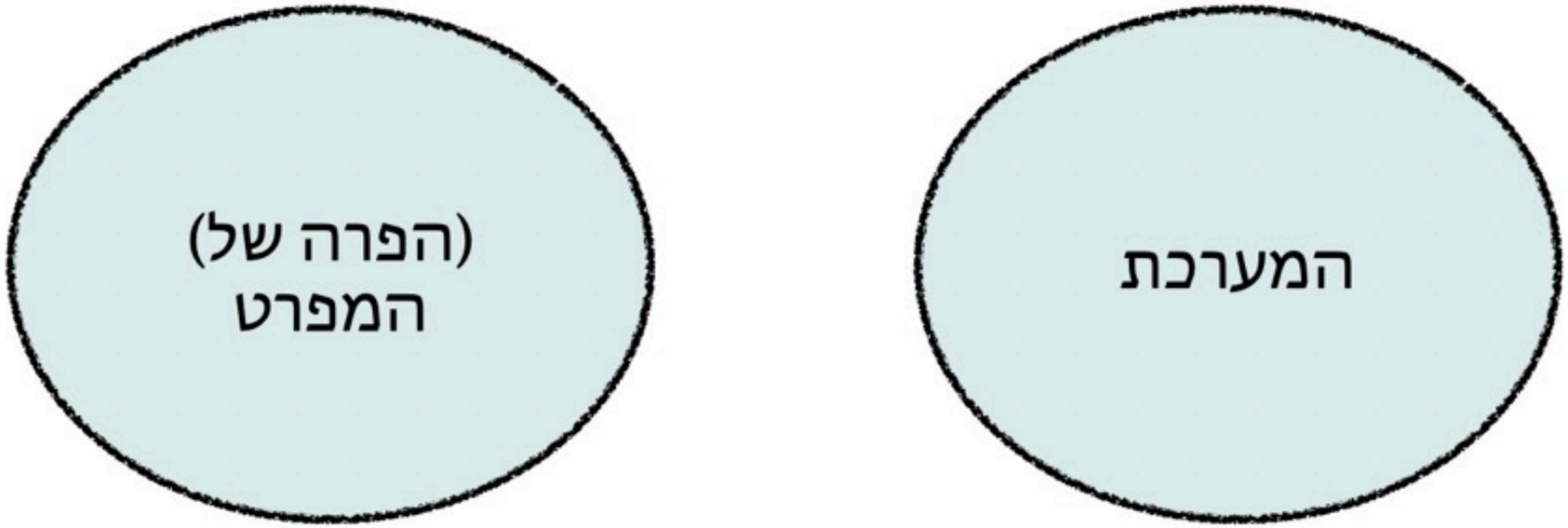


האם התכנית מספקת את המפרט?



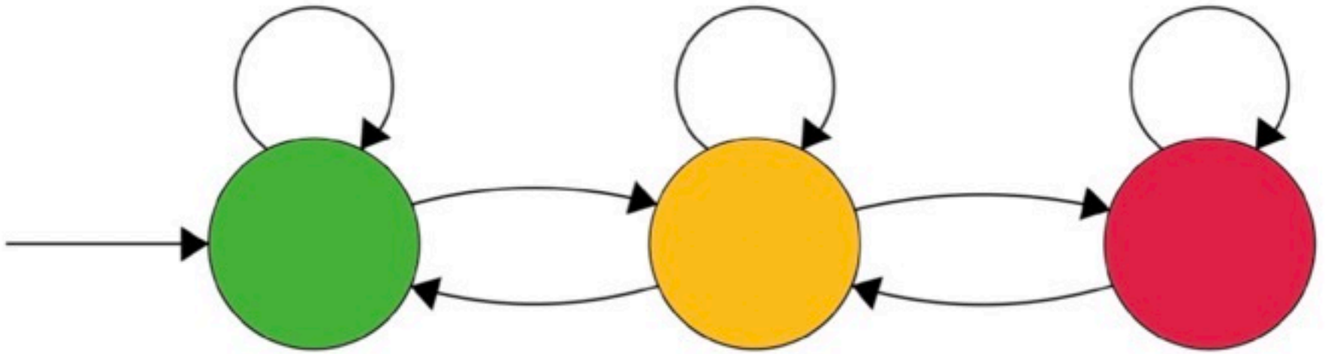
דוגמא לחישוב של המערכת
שמפר את המפרט

האם התכנית מספקת את המפרט?

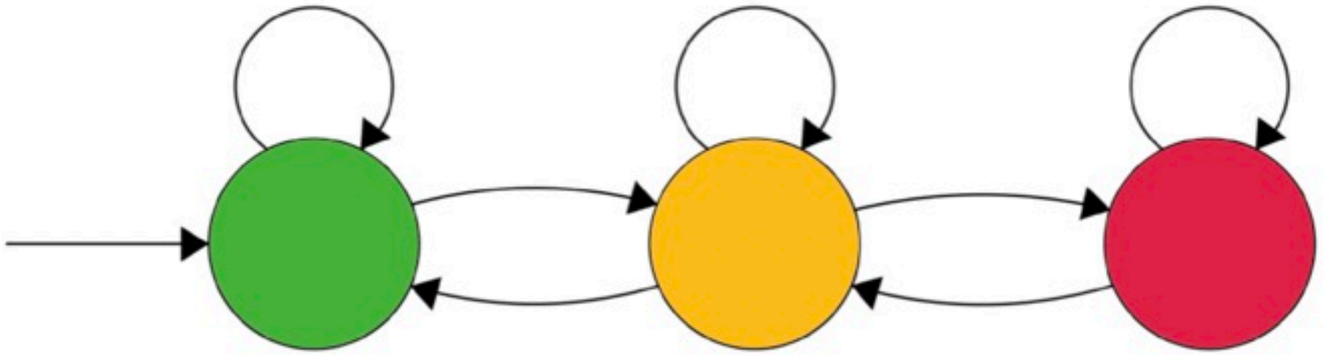


חיתוך ריק: הוכחה שהמערכת
מספקת את המפרט!

אוטומט (מכונת מצבים) עבור המערכת

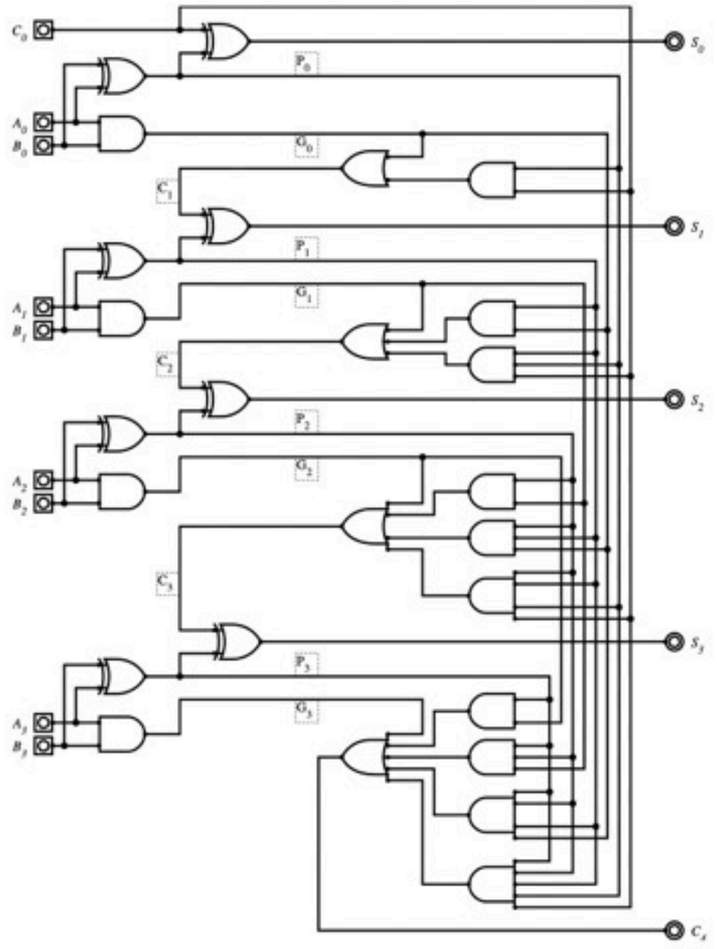


אוטומט (מכונת מצבים) עבור המערכת

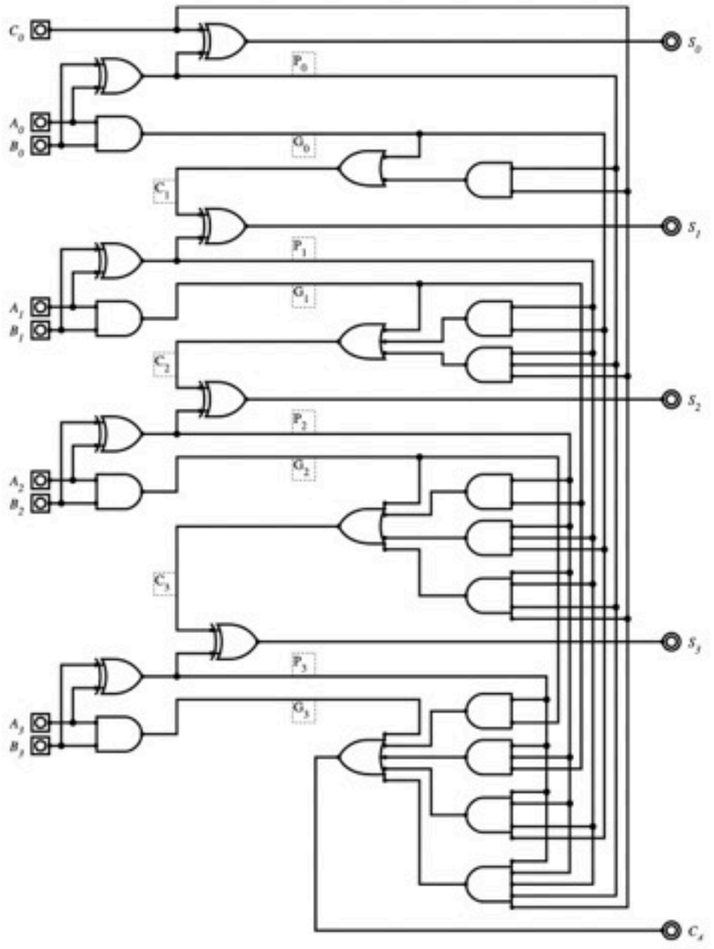


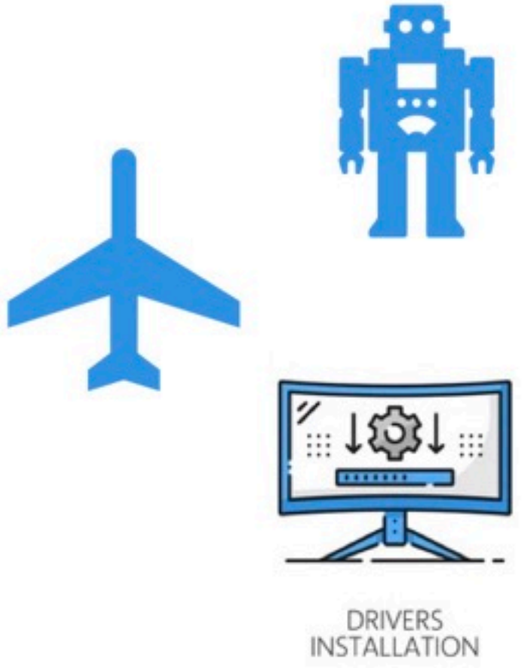
* מודל חישובי עם אלגוריתמים פשוטים עבור בעיות חשובות (למשל חיתוך)
* קשר ישיר ללוגיקה

אפשר למדל לא רק רמזורים!



אפשר למדל לא רק רמזורים!





אוטומט עבור (הפרה של) המפרט

המפרט: תמיד, בסופו של דבר האור יתחלף לירוק

אוטומט עבור (הפרה של) המפרט

המפרט: תמיד, בסופו של דבר האור יתחלף לירוק

הפרה של המפרט: בסופו של דבר, אף פעם האור לא ירוק

אוטומט עבור (הפרה של) המפרט

המפרט: תמיד, בסופו של דבר האור יתחלף לירוק

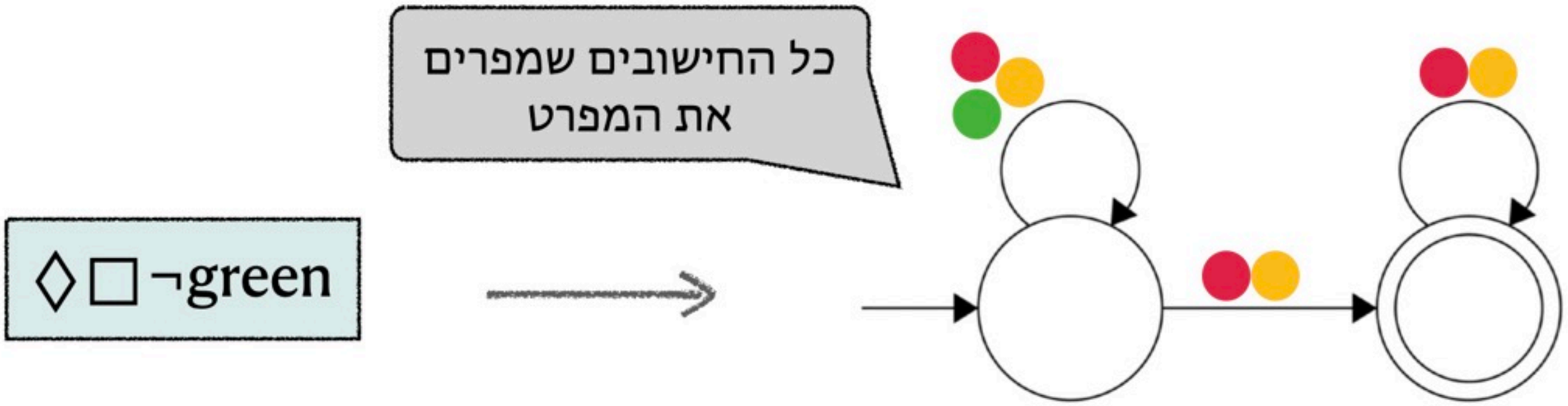
הפרה של המפרט: בסופו של דבר, אף פעם האור לא ירוק

$$\Diamond \Box \neg \text{green}$$

אוטומט עבור (הפרה של) המפרט

המפרט: תמיד, בסופו של דבר האור יתחלף לירוק

הפרה של המפרט: בסופו של דבר, אף פעם האור לא ירוק



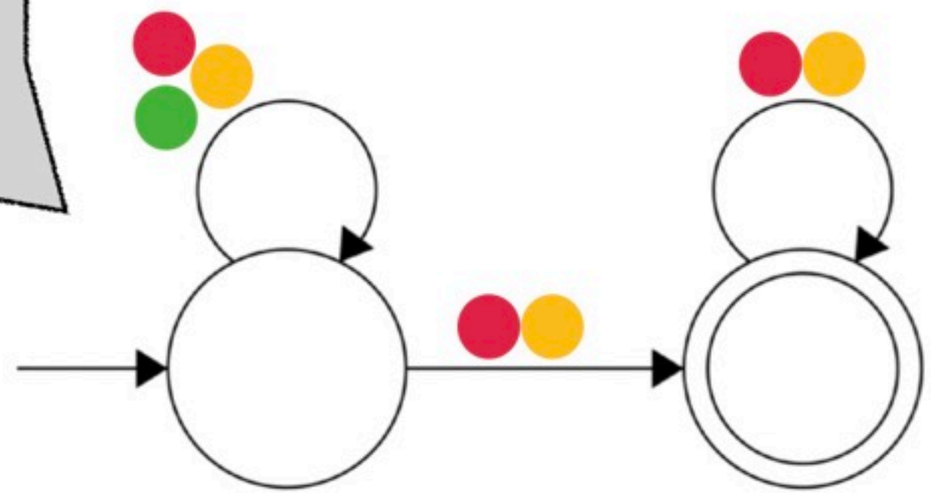
אוטומט עבור (הפרה של) המפרט

לוגיקה (שפה מתמטית) ⟵ אוטומט (מודל מתמטי עבור אלגוריתמים)

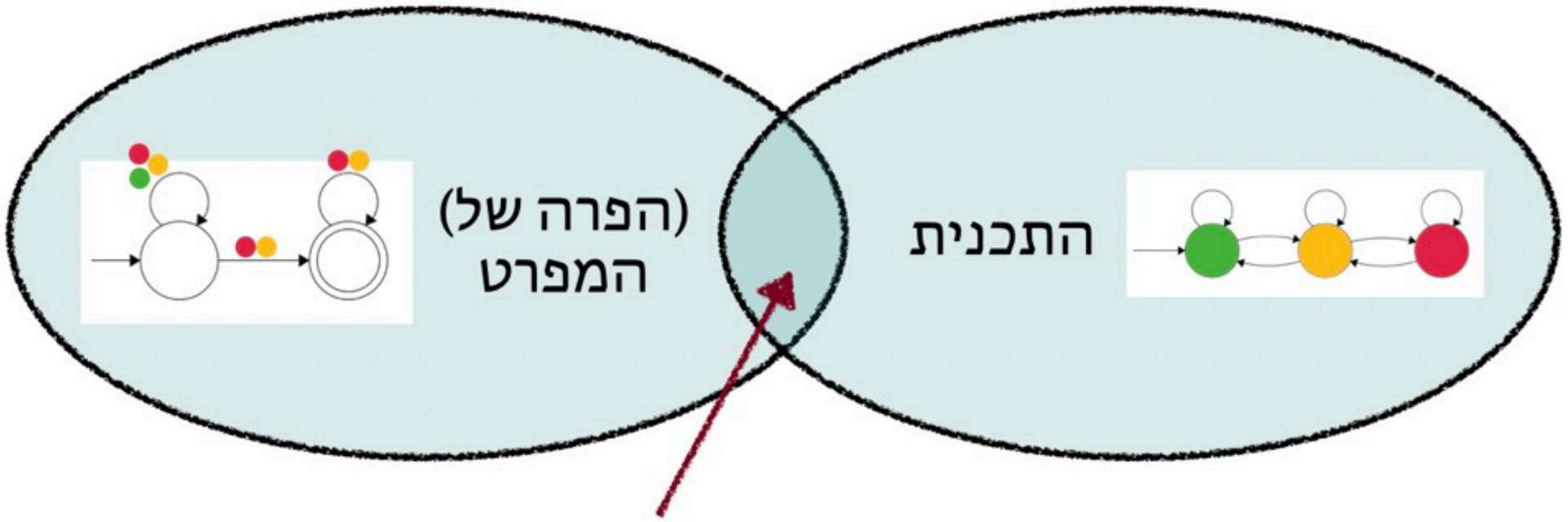
הפרה של המפרט: <u>בסופו של דבר, אף פעם</u> האור לא ירוק

כל החישובים שמפרים
את המפרט

$\Diamond\Box\neg green$



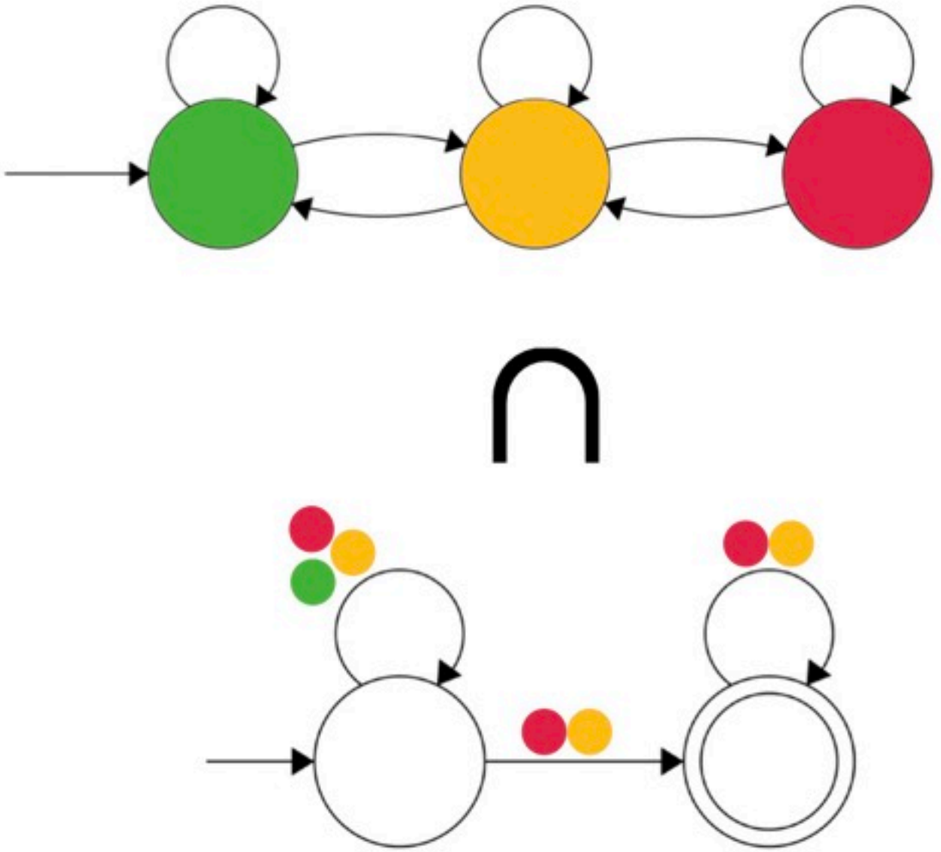
האם התכנית מספקת את המפרט?



דוגמא לחישוב של התכנית
שמפר את המפרט?

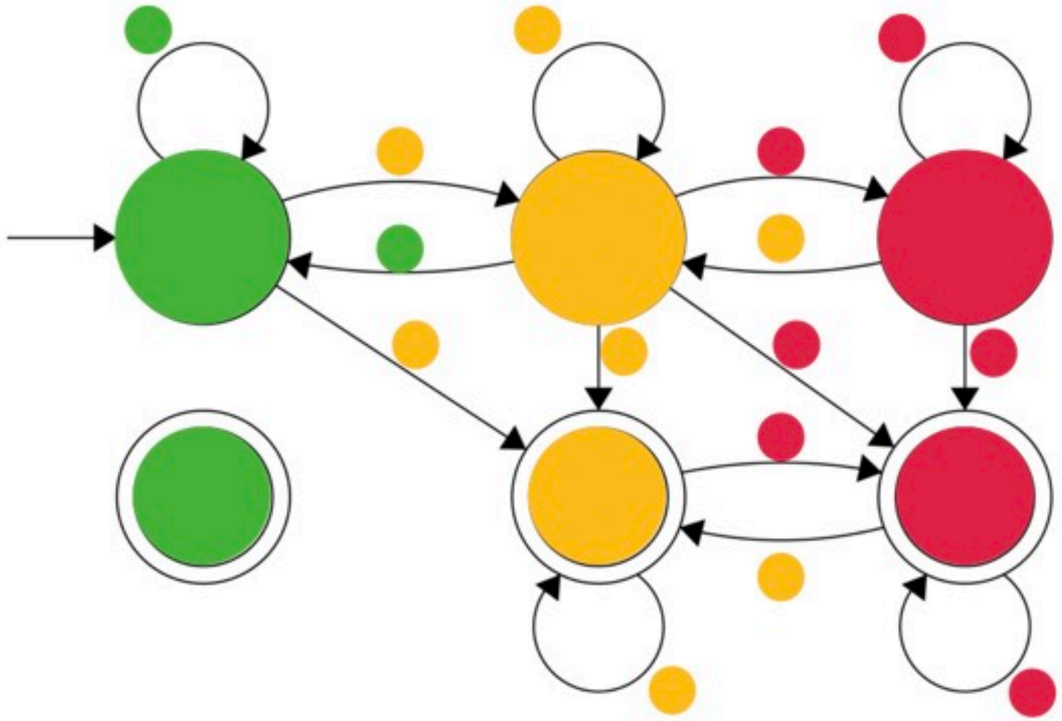
האם התכנית מספקת את המפרט?

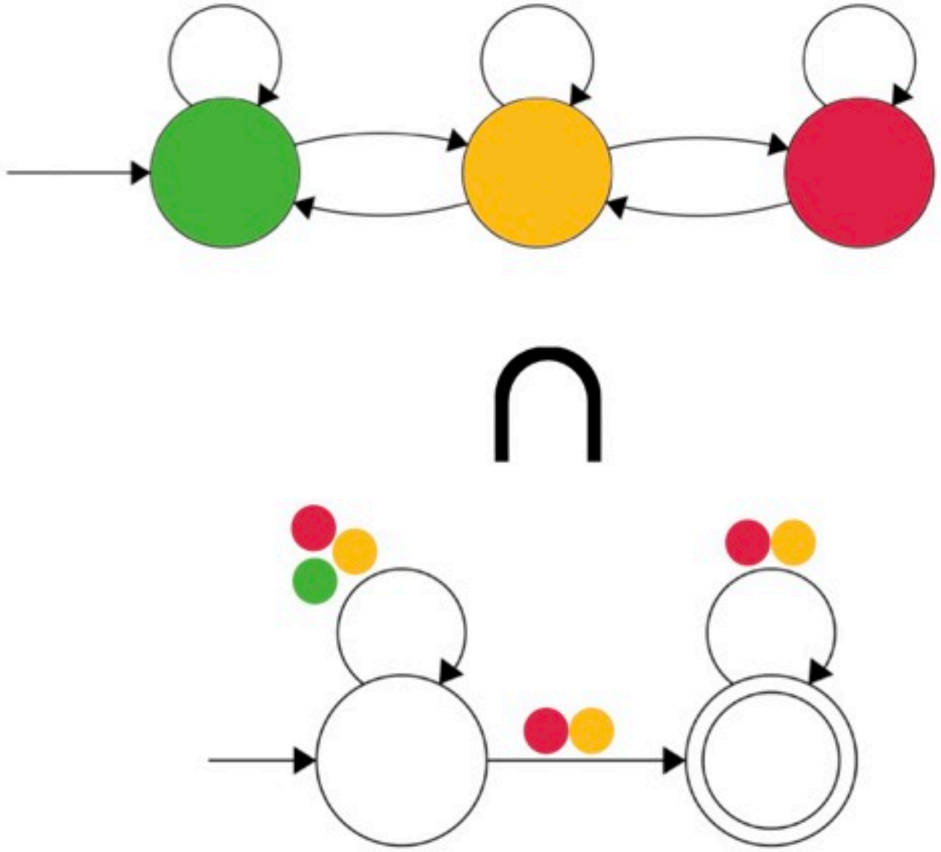
מחפשים חישובים של המערכת, שגם מפרים את המפרט



האם התכנית מספקת את המפרט?

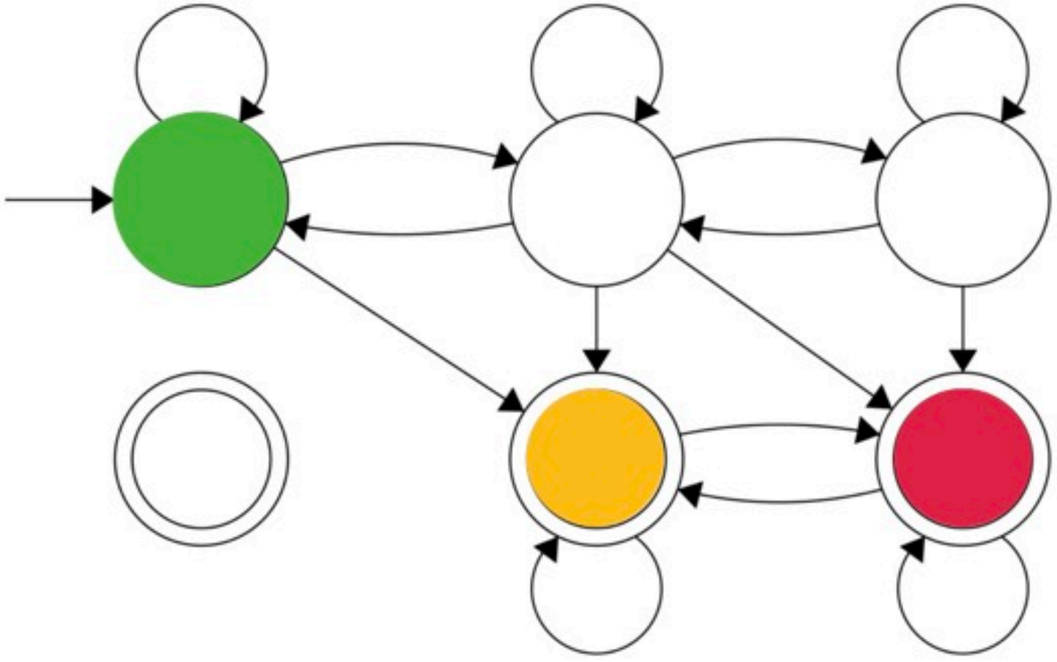
מחפשים חישובים של המערכת, שגם מפרים את המפרט

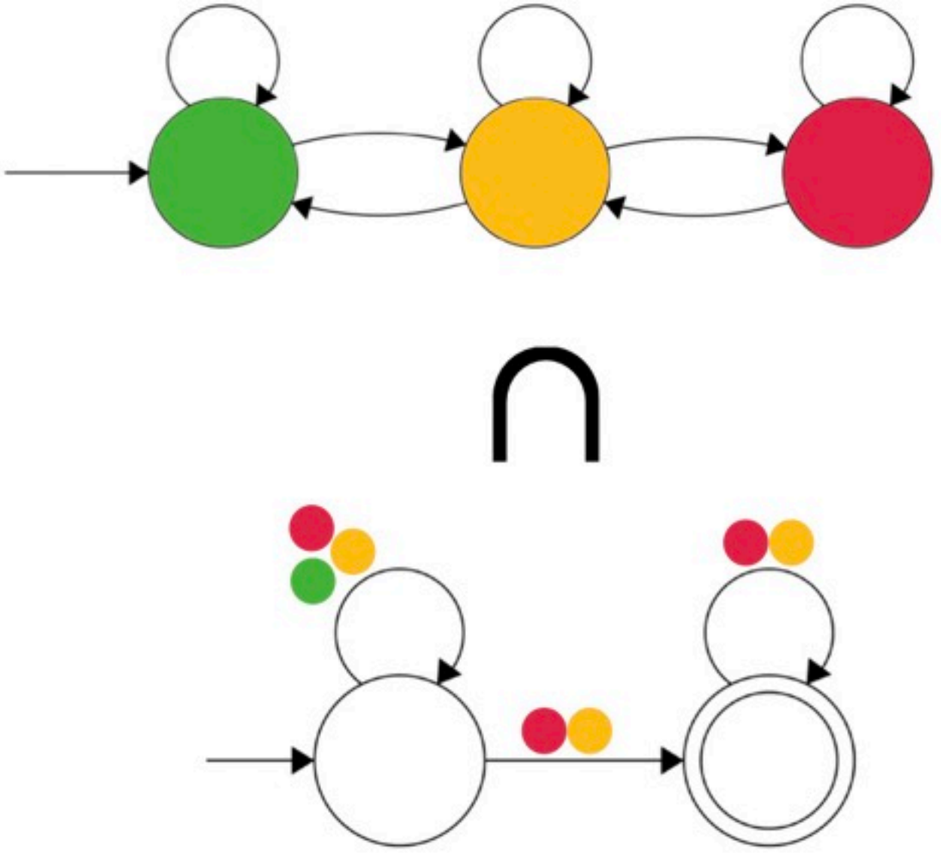




האם התכנית מספקת את המפרט?

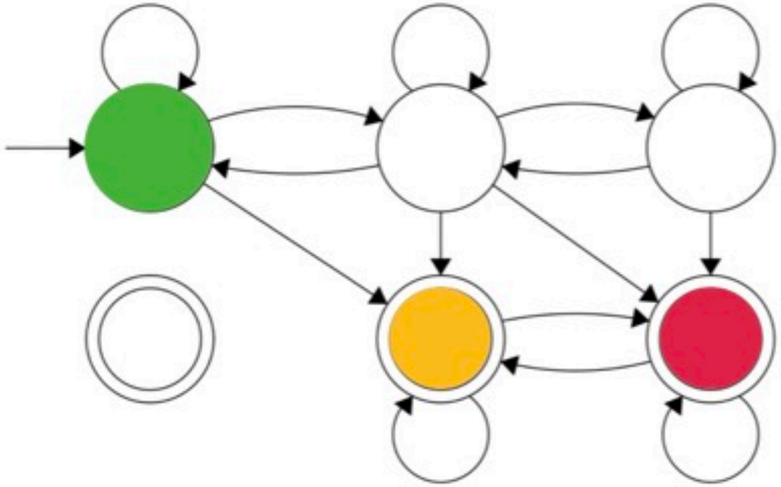
מחפשים חישובים של המערכת, שגם מפרים את המפרט

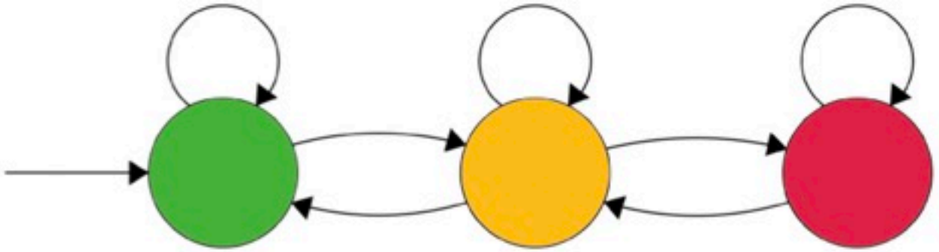


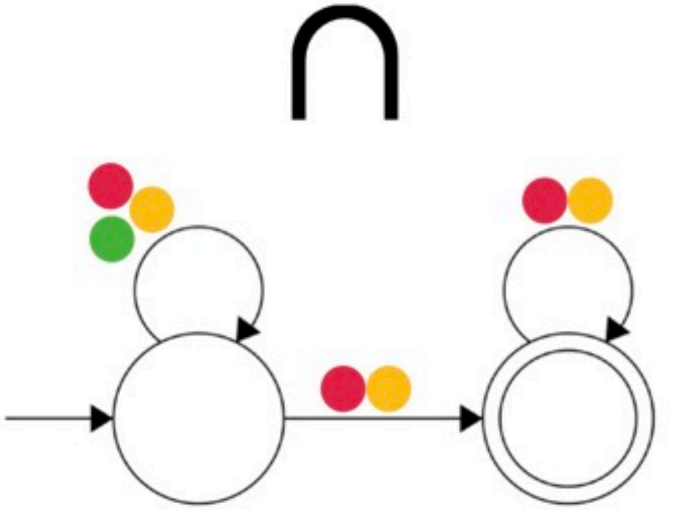


האם התכנית מספקת את המפרט?

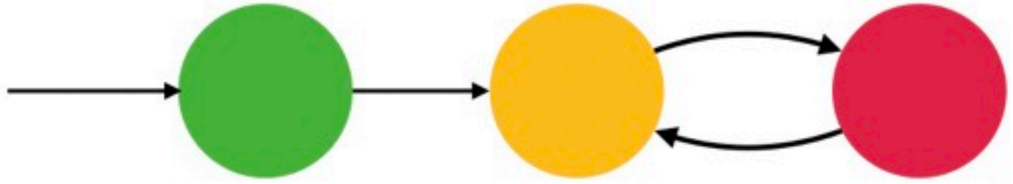
מחפשים חישובים של המערכת, שגם מפרים את המפרט





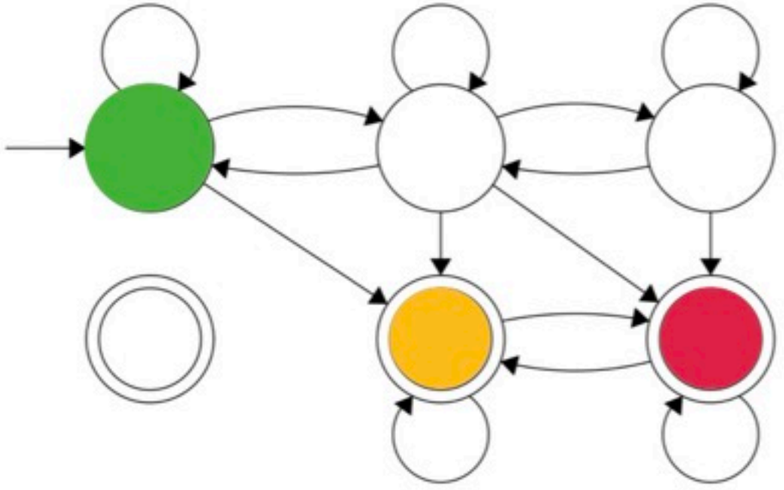


חישוב של המערכת בו נתקעים לנצח בלי אור ירוק

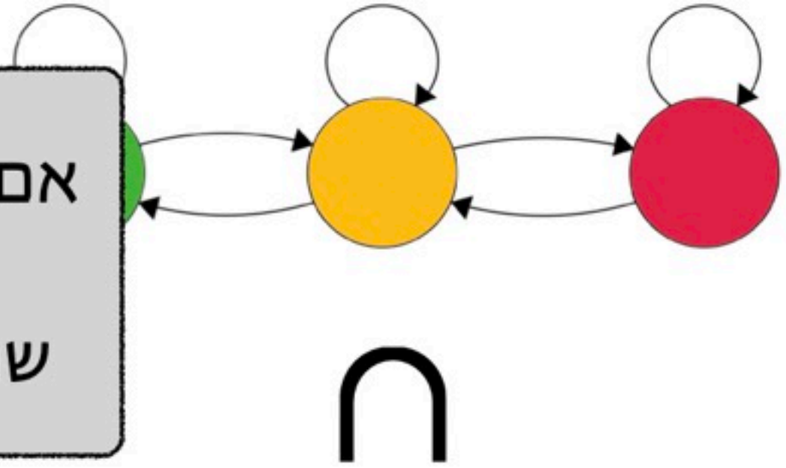


האם התכנית מספקת את המפרט?

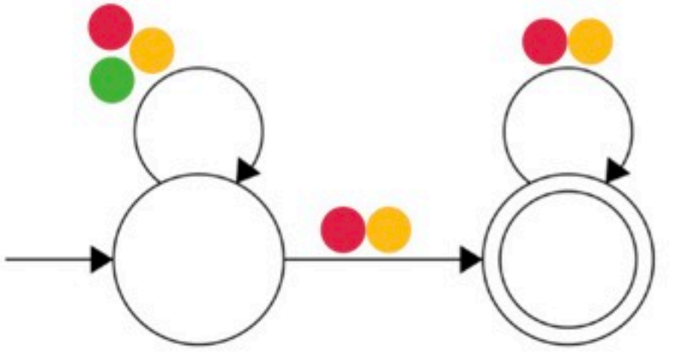
מחפשים חישובים של המערכת, שגם מפרים את המפרט



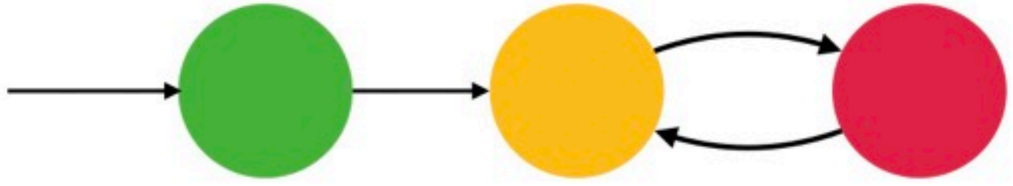
אם לא קיים חישוב כזה, הוכחנו שהתכנית נכונה!



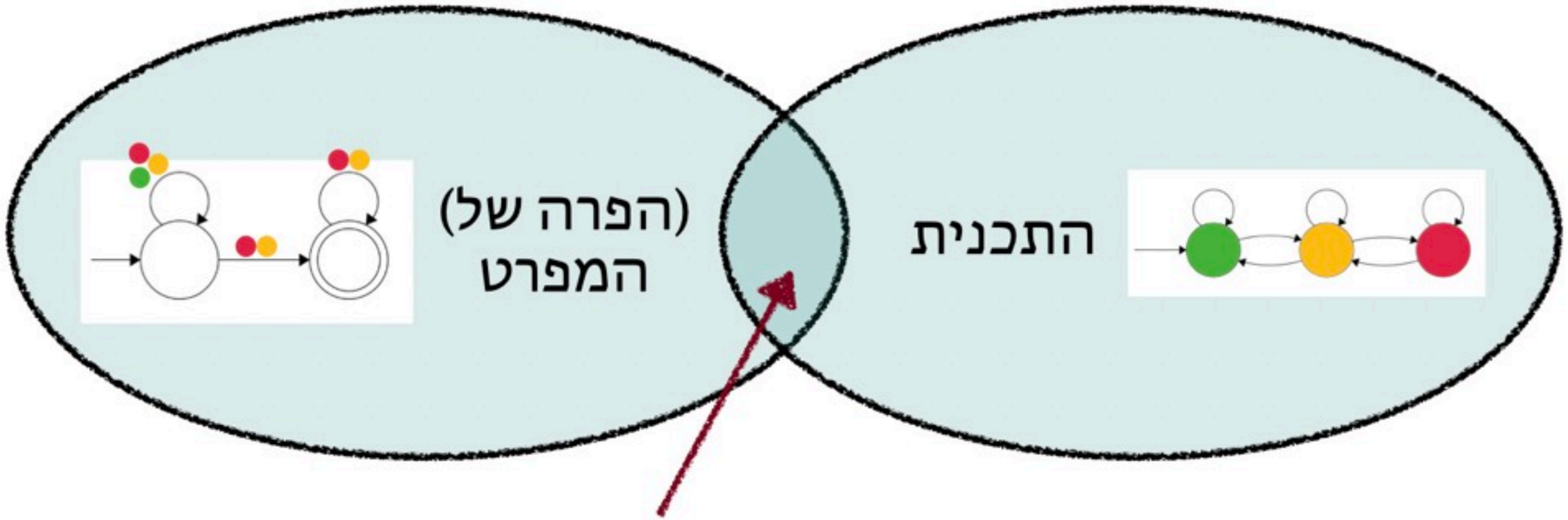
∩



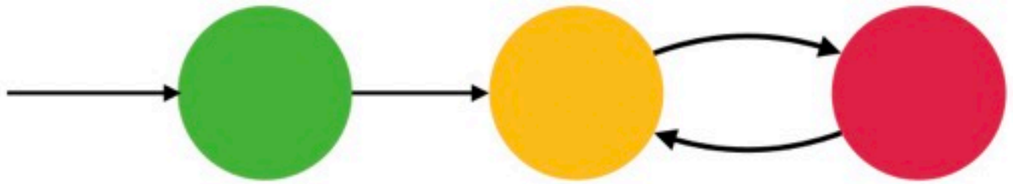
חישוב של המערכת בו נתקעים לנצח בלי אור ירוק



האם התכנית מספקת את המפרט?

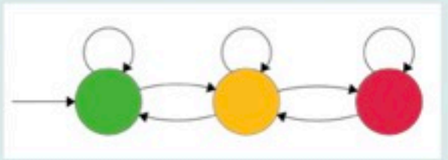


חישוב של המערכת בו נתקעים לנצח בלי אור ירוק

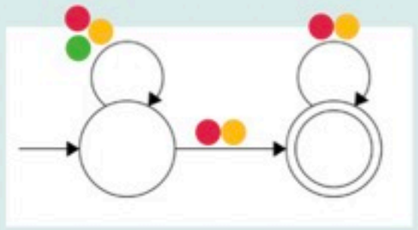


האם התכנית מספקת את המפרט?

התכנית



(הפרה של)
המפרט



אם החיתוך ריק,
הוכחנו שהתכנית
נכונה*!

לא רק רמזורים!

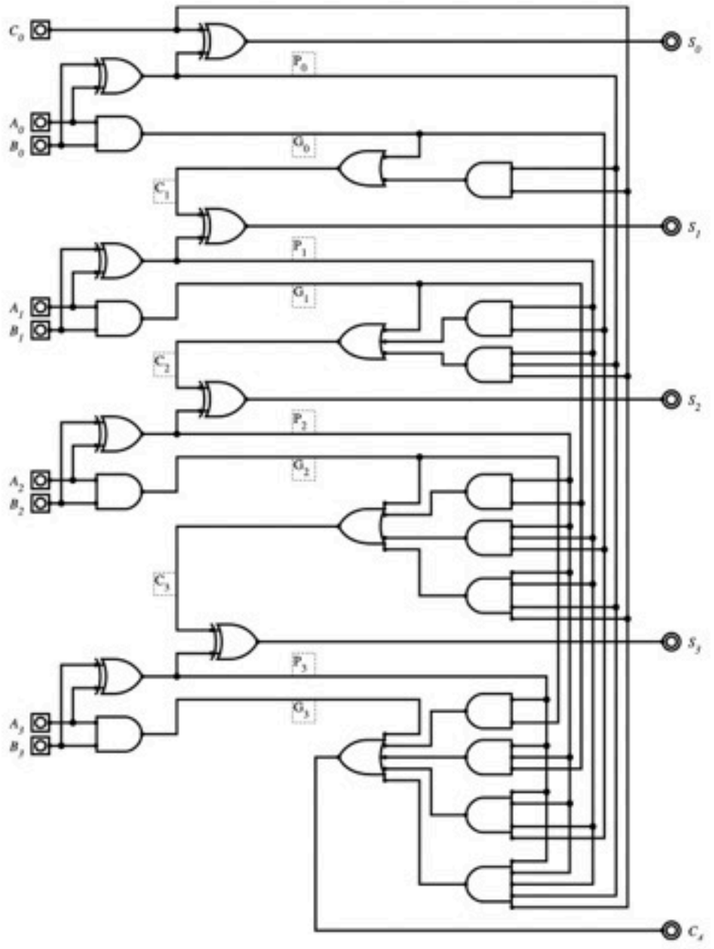
intel

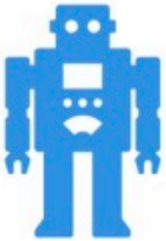
Windows

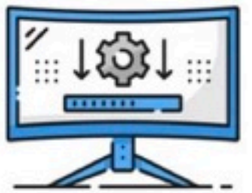
AIRBUS

NVIDIA

NASA







DRIVERS
INSTALLATION

מה עוד נשאר לעשות?

אימות פורמלי

לוקח **המון** זמן חישוב

עובד טוב על תכניות קטנות

מה עוד נשאר לעשות?

אימות פורמלי

לוקח **המון** זמן חישוב

עובד טוב על תכניות קטנות

מה עוד נשאר לעשות?

אימות פורמלי

לוקח **המון** זמן חישוב

עובד טוב על תכניות קטנות

המטרה: להצליח לטפל בתכניות גדולות יותר ויותר

ובטווח רחב יותר של תכניות

מה עוד נשאר לעשות?

לוגיקה!

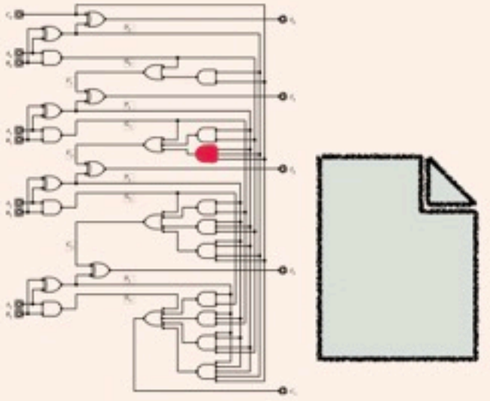
מה עוד נשאר לעשות?

לוגיקה!

$$\forall \pi_1 \forall \pi_2 \exists \pi_3 \,.\, (\pi_1 =_{\text{high-in}} \pi_3) \wedge (\pi_2 =_{\text{low-out}} \pi_3)$$

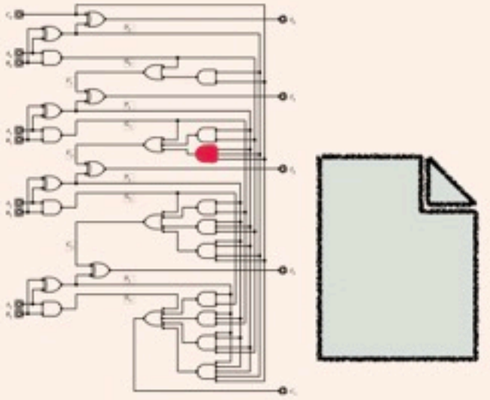
לוגיקה באימות פורמלי

- מאפשרת לנו להביע תכונות מעניינות על מחשבים
- **מאפשרת לנו להוכיח שתכניות נכונות!**



לוגיקה באימות פורמלי

- מאפשרת לנו להביע תכונות מעניינות על מחשבים
- **מאפשרת לנו להוכיח שתכניות נכונות!**

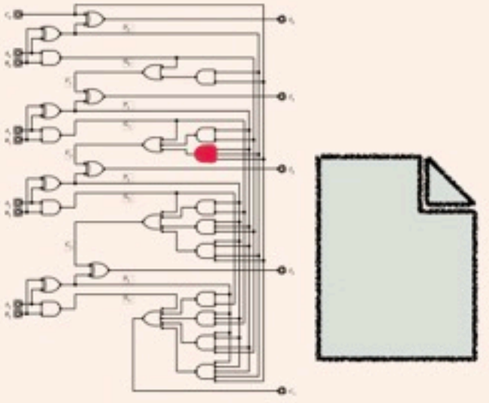


- להצליח להוכיח נכונות של תכניות גדולות יותר ובטווח רחב יותר של תכניות
- להצליח להביע את מגוון התכונות שמעניינות אותנו

תודה!

* אף חתול סגול מעופף לא נפגע בהכנת מצגת זו

- מאפשרת לנו להביע תכונות מעניינות על מחשבים
- **מאפשרת לנו להוכיח שתכניות נכונות!**



- להצליח להוכיח נכונות של תכניות גדולות יותר ובטווח רחב יותר של תכניות
- להצליח להביע את מגוון התכונות שמעניינות אותנו