The Clean Paper

WHAT THE PAPER SAYS · WHAT IT DOESN’T · WHY IT MATTERS

Cryptographic proof የጎደለው simulator እንደሌለ ማረጋገጥን ከባድ በማድረግ ምስጢሩን ሊደብቅ ይችላል

Zero-knowledge proofs አንድ ሰው witness-ውን ሳይገልጥ statement ማረጋገጥ እንዲችል ያደርጋሉ። Classical theory በሙሉ ትርጉሙ አንድ message፣ no trusted setup እና perfect soundness አብረው ሊኖሩ እንደማይችሉ ይላል። የRahul Ilango paper ያ impossibility እንዲጠፋ አያደርግም። Target-ውን ይቀይራል፡- simulator በእውነት እንዲኖር ከመጠየቅ ይልቅ፣ የተመረጠ proof system simulator እንደሌለ በብቃት ማረጋገጥ እንዳይችል ይጠይቃል። በትልቅ proof-complexity እና cryptographic assumptions ስር ይህ falsifiable፣ game-based consequences of zero-knowledgeን property በproperty ለማግኘት በቂ ነው። ነጥቡ plug-in internet primitive አይደለም፤ mathematical unprovabilityን ወደ cryptographic cover የሚቀይር proof-theoretic መንገድ ነው።

Written by Cinzia Vaglio · Cross-checked by Vera Rubin · Edited by Michele Renda · Figures by Nova Vela · AI-assisted, human-reviewed

Paper: *Gödel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness*, Rahul Ilango, FOCS 2025 / IACR ePrint 2025/1296 · DOI: 10.1109/FOCS63196.2025.00058

ዘዴው ምስጢሩ ተደብቋል ብሎ ማረጋገጥ አይደለም

ከዜሮ-እውቀት በጣም ቀላል ቅጂ እንጀምር።

አሊስ አንድ ሱዶኩ እንቆቅልሽ መፍትሔ እንዳለው ቦብን ማሳመን ትፈልጋለች። መፍትሔውን ከላከችለት ቦብ ይረጋገጣል፣ ግን እንቆቅልሹ ይበላሻል። የምትፈልገው ይበልጥ እንግዳ ነገር ነው፦ መፍትሔውን ሳትገልጥ መፍትሔ እንዳለ የሚያረጋግጥ ማረጋገጫ።

ይህ የዜሮ-እውቀት ማረጋገጫ ተስፋ ነው። ማስረጃ አቅራቢው (አሊስ) አባባሉ እውነት መሆኑን አረጋጋጭ-ውን (ቦብ) ያሳምናል፣ ከአባባሉ እውነት በላይ ምንም ሳይገልጥ።

ችግሩ ይህ ተስፋ ዋጋ መኖሩ ነው። መደበኛ የሒሳብ ማረጋገጫ ሁለት ምቹ ባህሪያት አሉት። አንድ መልዕክት ነው፦ ይጽፉታል፣ ይሰጡታል፣ ይሄዳሉ። እና ፍጹም ትክክል ነው፦ ሐሰተኛ አባባል ምንም ትክክለኛ ማረጋገጫ የለውም። ክላሲካል የማይቻልነት ውጤቶች ዜሮ-እውቀት ሁለቱንም ባህሪያት መተው እንዳለበት ይላሉ — ሁለቱን አብሮ ብቻ አይደለም፤ እያንዳንዳቸውም ብቻውን አይቻልም።

መጀመሪያ፣ ዜሮ-እውቀት ማረጋገጫ ውይይት ይፈልጋል። አሊስ አንድ መልዕክት ብቻ ከላከች፣ አስቀድሞ የተዘጋጀ የታመነ ቅድመ-ዝግጅት ከሌለ፣ ዜሮ-እውቀት ዋስትናው ይወድቃል — እና በምትኩ ትክክለኛነትን ምን ያህል ለመቀነስ ፈቃደኛ ቢሆኑም ይህ ይሠራል።

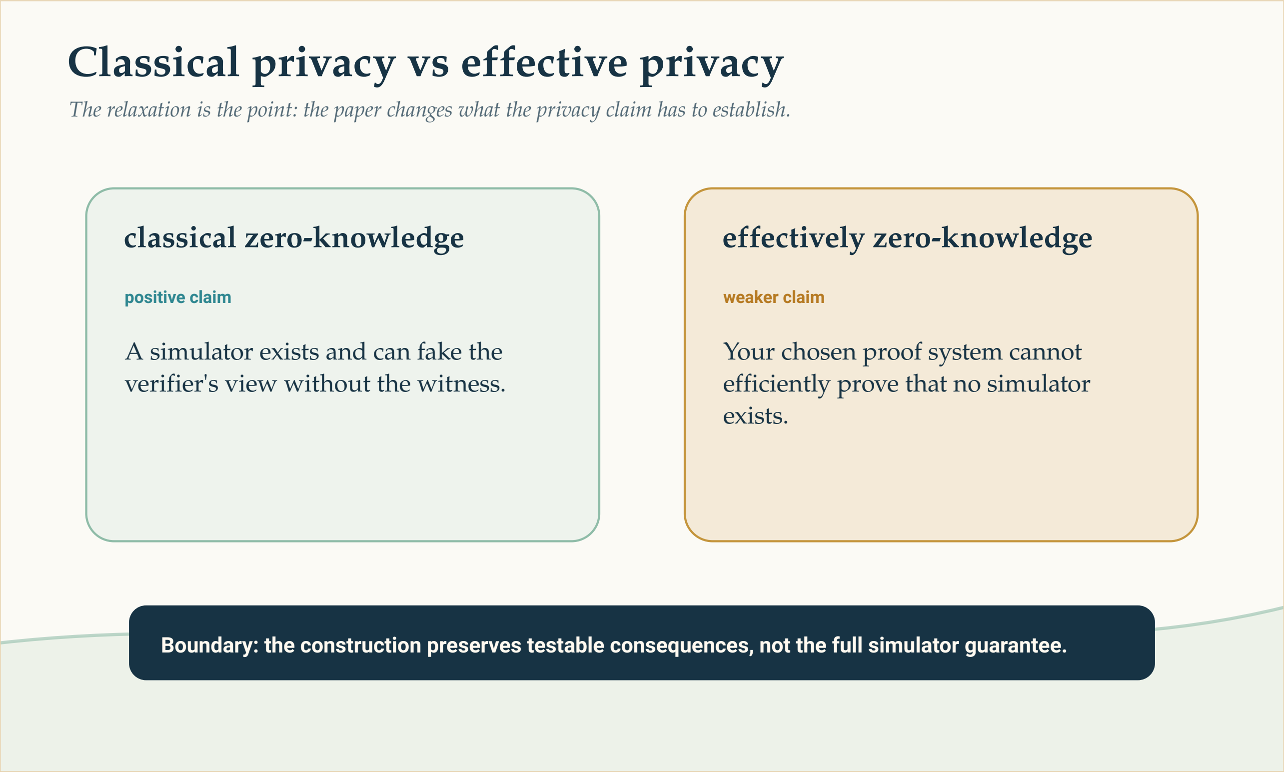
ሁለተኛ፣ ዜሮ-እውቀት ማረጋገጫ ትንሽ የስህተት መቻቻል ይፈልጋል። Perfect ትክክለኛነትን መጠየቅ በዝምታ መስተጋብር-ንም ያጠፋል፦ አረጋጋጭ ምንም የዘፈቀደ ምርጫዎች ቢያደርግ ፈጽሞ ሊታለል የማይችል ከሆነ፣ እነዚያ ምርጫዎችን አስቀድሞ መወሰን ይችላል። አረጋጋጭ-ው ከተገመተ በኋላ አሊስ ሁሉንም መልስ በአንድ መልዕክት ማስገባት ትችላለች — ይህም ቀድሞውኑ የተበላሸው ነገር ነው።

የRahul Ilango ወረቀት ይህን ሁለት ድርብ ግድግዳ ለማለፍ የሚሞክር መንገድ ነው። ግድግዳው የለም ብሎ በመምሰል አይደለም፣ እና በክላሲካል ትርጉም የማይቻለውን ዜሮ-እውቀት በዚያ ሁኔታ እንዳለ በማቅረብ አይደለም። እርምጃው ይበልጥ ስውር ነው፦ “ምንም አይገልጥም” የሚለውን ትርጉም ያደክማል፣ ግን cryptographers በእውነት ሊፈትኗቸው የሚችሉ የደህንነት ባህሪያትን በሚጠብቅ መንገድ።

ውጤቱ በተግባር ዜሮ-እውቀት ይባላል።

ዜሮ-እውቀት በሶስት በሮች ላይ ታግዷል — መስተጋብር፣ የታመነ ቅድመ-ዝግጅት እና imፍጹም ትክክለኛነት። የIlango ግንባታ ግን በሌላ በር ይወጣል፦ የደንብ ሥርዓቱ አስመሳዩን በብቃት ማስተባበል አይችልም።

Original diagram — The Clean Paper CC BY 4.0



ክላሲካል ዜሮ-እውቀት አስመሳይ በእውነት አለ ወይ? ብሎ ይጠይቃል፤ “በተግባር ዜሮ-እውቀት” ግን የመረጡት የደንብ ሥርዓት አስመሳይ እንደሌለ በብቃት ማረጋገጥ ይችላል ወይ? ብቻ ይጠይቃል። ይህ ደካማ ጥያቄ ነው ግንባታውን አንድ መልዕክት፣ ያለ

ቅድመ-ዝግጅት እና ፍጹም ትክክለኛነት እንዲያቆይ የሚያስችለው።

Original diagram — The Clean Paper CC BY 4.0

አሮጌው ፈተና፡- አስመሳይ በእውነት አለ

ዜሮ-እውቀትን በክላሲካል መንገድ ለመደበኛ ማድረግ አስመሳይ የሚባል ምናባዊ ረዳት ይጠቀማል።

ሐሳቡ ይህ ነው፡- ጄን የአሊስ ምስጢርን **አታውቅም** እንበል። ጄን ብቻዋን ሆና ቦብ ከአሊስ ሊቀበላቸው ከነበሩት ማረጋገጫዎች ጋር ተመሳሳይ የሚመስሉ ማረጋገጫዎች ማመንጨት ከቻለች፣ የአሊስ ማረጋገጫዎች ቦብን አዲስ ነገር አላስተማሩትም ማለት ነው። ጄን የአሊስ ምስጢር ሳይኖራት ያንን ልምድ ቀድሞውኑ ማስመሰል ትችላለች።

ስለዚህ ክላሲካል ዜሮ-እውቀት እውነተኛ አስመሳይ ይፈልጋል። ምስጢሩን — በየባለሙያ ቃል ምስክር፣ ለሱዶኩ ደግሞ በቀላሉ የተፈታ ፍርግርግ — ሳያውቅ እውነተኛ ማረጋገጫዎች የሚመስሉ ነገሮችን ማመንጨት የሚችል ውጤታማ አልጎሪዝም መኖር አለበት።

ያ ትርጉም ኃይለኛ ነው፣ ግን አሮጌው የማይቻልነት ትክክለኛው የሚመታውም እዚያ ነው። ስሜቱ ይህ ነው፡- በእውነት መስተጋብር-አልባ ማረጋገጫ አንድ ሕብረቁምፊ ብቻ ነው። ቦብ ያንን ሕብረቁምፊ ካገኘ በኋላ ለሌላ ሰው ማሳየት ይችላል፤ አባባሉን ለሌሎች ማረጋገጥ የሚችል ኃይል አግኝቷል፤ ይህም ከ“ምንም አልተማረም” በላይ ይመስላል። ክላሲካል ቲዎረሞች ይህን ግንዛቤ ወደ ላይ የተጠቀሱት የማይቻልነት ውጤቶች ያጠናክራሉ።

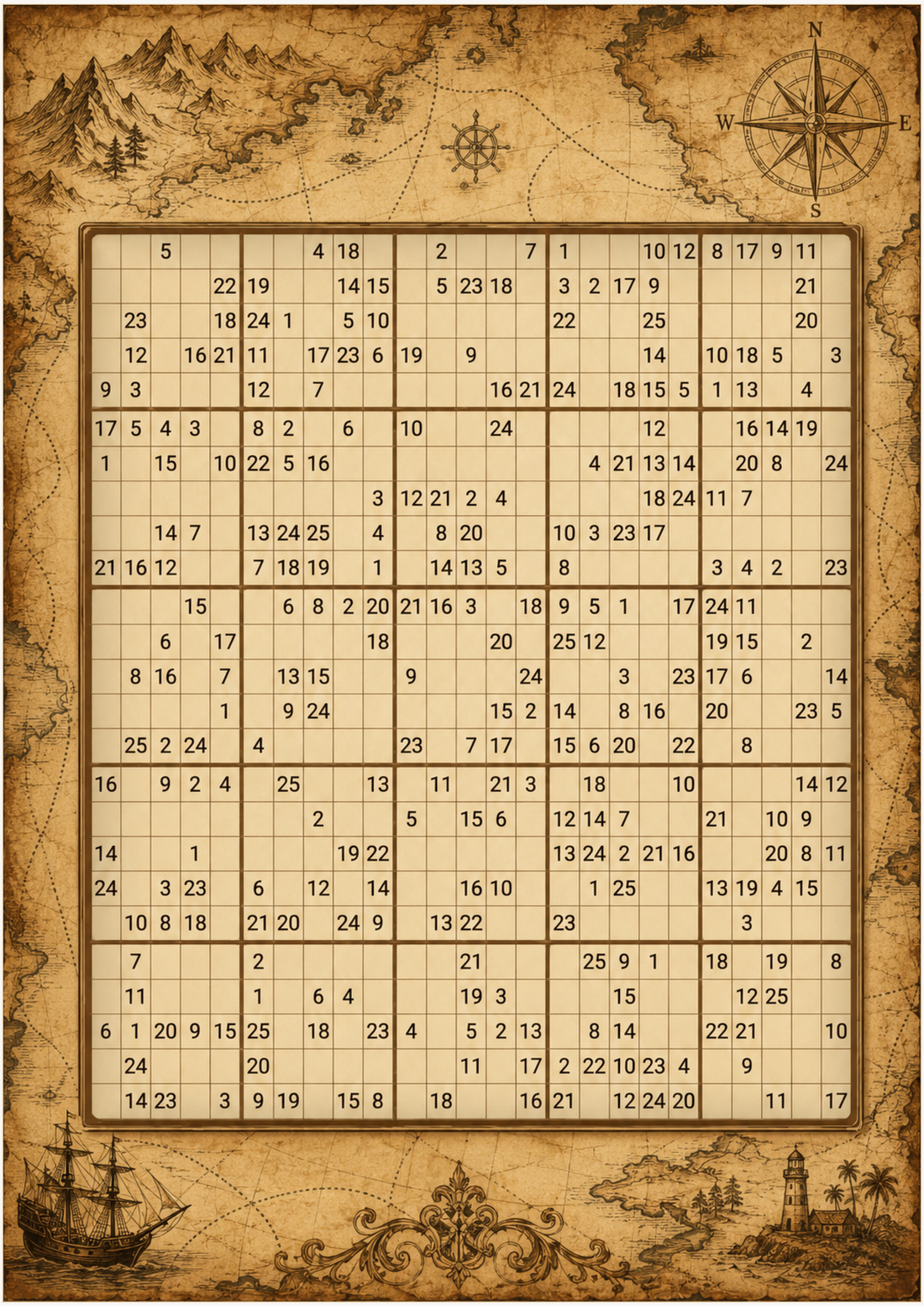
> **ይህ ወረቀት የማይተዋቸው ሶስት ባህሪያት**
>
> የጽሑፍ ርዕስ ሶስት ገደቦች ይጠራል፡-
> **መስተጋብር የለም፡-** አሊስ አንድ ማረጋገጫ ሕብረቁምፊ ትልካለች። ወደፊትና ወደኋላ የሚካሄድ ፕሮቶኮል የለም።
> **ቅድመ-ዝግጅት የለም፡-** አሊስ እና ቦብ የታመነ የተለመደ ማጣቀሻ ሕብረቁምፊ ወይም አስቀድሞ በተዘጋጀ የጋራ የዘፈቀደ መረጃ ላይ አይተማመኑም። “Non-interactive ዜሮ-እውቀት” የሚባሉ ብዙ ሥርዓቶች አሁንም ቅድመ-ዝግጅት ይፈልጋሉ፤ ይህ ወረቀት ያለ **ቅድመ-ዝግጅት** ማለት ነው።
> Perfect **ትክክለኛነት፡-** ሐሰተኛ አባባል ምንም ትክክለኛ ማረጋገጫ የለውም። “በጣም አልፎ አልፎ ብቻ ይቀበላል” አይደለም፤ ትክክለኛ ማረጋገጫ ፈጽሞ የለም።
> እነዚህ ሶስት ባህሪያት መደበኛ የተጻፈ ሒሳብ ያለው ትክክለኛ ባህሪ ነው — እና ከላይ እንደተገለጸው ክላሲካል ዜሮ-እውቀት እነሱን ሁሉ ማቆየት አይችልም።

ልዩነቱን በሜጋ-ሱዶኩ ማሰብ

ልዩነቱን ለማሰብ በዓላማ የቀለለ ምሳሌ እንይ።

ከባዱ ክፍል ላይ መደበኛ 9-by-9 ሱዶኩ አንጠቀም። በጣም ትንሽ እና በጣም ውሱን ነው፤ ኮምፒውተር በቀጥታ ሊፈታው ወይም መፍትሔ እንደሌለው ሊያረጋግጥ ይችላል። በምትኩ **ሜጋ-ሱዶኩ**(n) እንቆቅልሾች ቤተሰብ እንዳለ ያስቡ። መደበኛውን ደንብ እናስፋፋ፡- ክፍል size n ይምረጡ፣ $N = n \wedge 2$ ያድርጉ፣ እና N በ N ፍርግርግ ይገንቡ፣ ወደ n በ n ክፍሎች የተከፈለ፣ N ምልክቶች ያሉት። መደበኛ ሱዶኩ ትንሹ $n = 3$, $N = 9$ ሁኔታ ብቻ ነው፡- 9-by-9 ፍርግርግ፣ 3-by-3 ክፍሎች እና 9 ምልክቶች። ማረጋገጫ-ውስብስብነት ታሪኩ n ሊያድግ ሲችል፣ እና ፍርግርግ-ው

SAT ቀመር እንደ ሱዶኩ የተለበሰ እንዲሠራ የሚያደርጉ ተጨማሪ ረዳት አወቃቀሮች ሊይዝ ሲችል ነው የሚጀምረው። SAT ቀመር በቀላሉ የyes/no ገደቦች ዝርዝር ነው፦ ተለዋዋጮች-ን እውነት/ሐሰት አድርገን እያንዳንዱ ገደብ እንዲሟላ ማድረግ እንችላለን?



25x25 ሱዶኩ፦ የተጠናቀቀውን ፍርግርግ — ምስክሩን — ሳያሳይ ህጎቹ ሊመረመሩ ይችላሉ፤ የተደበቀ መፍትሔ እንዳለ የሚያረጋግጥ ማረጋገጫ ምሳሌ።

AI-generated editorial thumbnail — The Clean Paper CC BY 4.0

ሱዶኩ እና SAT፦ አንድ ችግር በሁለት ልብስ

ሱዶኩ “እንደ SAT ቀመር ሊሠራ” ይችላል የሚለው ምሳሌ ብቻ አይደለም። Translation-ው በሁለቱም አቅጣጫ ይሠራል፤ ቀላሉ አቅጣጫም በሙሉ ሊጻፍ ይችላል።
ከሱዶኩ ወደ SAT። SAT እውነት/ሐሰት ብቻ ይናገራል፤ ስለዚህ ለእያንዳንዱ (ረድፍ, ዓምድ, እሴት) ሶስትዮሽ አንድ ቡሊያን ተለዋዋጭ እንስጥ፦ $x(r,c,v)$ ማለት “ረድፍ r፣ ዓምድ c ያለው ሴል እሴት v ይይዛል” ማለት ነው። 4-by-4 ሱዶኩ (2-by-2 ክፍሎች፣ እሴቶች 1–4) 4·4·4 = 64 ተለዋዋጮች ይፈልጋል፤ ክላሲካል 9-by-9 ደግሞ 729። እያንዳንዱ ሱዶኩ ደንብ ወደ ንዑስ አባባሎች ስብስብ ይቀየራል። (ንዑስ አባባል የተለዋዋጮች ወይም negations-አቸው OR ነው፤ ሙሉ ቀመር የሁሉም ንዑስ አባባሎች AND ነው።)
እያንዳንዱ ሴል ቢያንስ አንድ እሴት ይይዛል — ለእያንዳንዱ ሴል አንድ ንዑስ አባባል፦

$$x(1,1,1) \lor x(1,1,2) \lor x(1,1,3) \lor x(1,1,4)$$

እያንዳንዱ ሴል ከአንድ በላይ እሴት አይይዝም — ለእያንዳንዱ የእሴቶች ጥንድ “ሁለቱም አይደሉም” ንዑስ አባባል፦

$\neg x(1,1,1) \lor \neg x(1,1,2)$ $\neg x(1,1,1) \lor \neg x(1,1,3)$ … እና በዚህ መልኩ ለሁሉም ስድስት ጥንዶች።

እያንዳንዱ ረድፍ እያንዳንዱን እሴት ይይዛል — ለረድፍ 1 እና እሴት 3፣ ቢያንስ አንድ ጊዜ፦

$$x(1,1,3) \lor x(1,2,3) \lor x(1,3,3) \lor x(1,4,3)$$

እና ቢበዛ አንድ ጊዜ፦ $\neg x(1,1,3) \lor \neg x(1,2,3)$፣ እና በረድፍ-ው ውስጥ ለእያንዳንዱ ጥንድ of ሴሎች እንዲሁ።
ዓምዶች እና ክፍሎች — ተመሳሳይ ስብስቦች፣ የሚቀየረው የሴሎች ቡድን ብቻ ነው። ለtop-left ክፍል እና እሴት 2፦

$$x(1,1,2) \lor x(1,2,2) \lor x(2,1,2) \lor x(2,2,2)$$

እና pairwise “not both” ንዑስ አባባሎች።
የታተሙ ፍንጮች — በጣም ቀላሉ ክፍል፦ እያንዳንዱ ፍንጭ አንድ ተለዋዋጭ ብቻ ያለው ንዑስ አባባል ነው። Top-left ጥግ ላይ የታተመ 3፦

$$x(1,1,3)$$

ይሆናል።
የዚህ ሁሉ AND በትክክል ሱዶኩ-ው መፍትሔ ሲኖረው ሊሟላ የሚችል ይሆናል — እና የሚያሟላ ምደባ ራሱ *መፍትሔው ነው*፦ የትኞቹ $x(r,c,v)$ እውነት እንደሆኑ ይመልከቱ እና ፍርግርግ-ውን ይሙሉ። ለ9-by-9 ይህ 729 ተለዋዋጮች እና ጥቂት ሺህ ንዑስ አባባሎች ይሆናል፤ ዘመናዊ SAT ፈቺ ፕሮግራም በሚሊሰከንዶች ይፈታዋል። ፍንጭ ንዑስ አባባል $x(1,1,3)$ ያስተውሉ፦ “ይህ ሴል በትክክል 3 ነው” ይላል፤ “እነዚህ ሴሎች ሁሉ የተለያዩ ናቸው” አይልም — ይህም ከታች በፕሮቶኮል note ውስጥ ፍንጭ ሴሎች ተጨማሪ ዘዴ የሚፈልጉበት ያው አለመመጣጠን ነው።
ከSAT ወደ ሱዶኩ። ጽሑፉ የሚፈልገው ተቃራኒው፣ ከባዱ አቅጣጫ ነው፦ አንድ የዘፈቀደ SAT ቀመር ተሰጥቶ፣ ቀመሩ መፍትሔ ካለው ብቻ መፍትሔ ያለው ሜጋ-ሱዶኩ መገንባት። ሱዶኩ የራሱ ደንቦች “እነዚህ ሴሎች ሁሉ የተለያዩ ናቸው” ብቻ ሊሉ ይችላሉ፣ ስለዚህ የዘፈቀደ ሎጂካዊ ገደቦች መገንባት አለባቸው — ይህ በትክክል ረዳት አወቃቀሮች የሚሠሩት ነው። ረዳት አወቃቀር ለቀመሩ እያንዳንዱ ንዑስ አባባል የተዘጋጀ ትንሽ ስብስብ

> of ሴሎች ነው፣ የተመደቡ ሴሎች የተለዋዋጮች ሚና ይጫወታሉ (የሚይዙት ምልክት እውነት ወይም ሐሰትን ይወክላል)፣ እና ስብስብ-ው ውስጣዊ ገደቦች የተቀናበሩት ንዑስ አባባል-ውን የሚያሟሉ ምደባዎች ብቻ የተፈቀደ ሙሌቶች እንዲሆኑ ነው። ይህ በNP-completeness ማረጋገጫዎች የተለመደ የግንባታ ዘዴ ነው፤ ለአጠቃላይ የተደረገ ሱዶኩ በ2003 Yato እና Seta አድርገውታል።
> ሁለቱ አቅጣጫዎች አብረው N-by-N ሱዶኩ እና SAT ተመሳሳይ ችግር በተለያዩ ልብሶች እንደሆኑ ይላሉ። ይህ ነው ይህ ጽሑፍ — እና ጽሑፉ — ፍርግርጎች እና ምልክቶች ተጠቅሞ ስለ NP ሁሉ ታሪክ እንዲናገር የሚፈቅደው።

ምስክሩን አሁንም በቀላሉ ማሰብ ይቻላል። አሊስ ሜጋ-ሱዶኩ-ውን ሙሉ በሙሉ ትክክል የሚሞላ መፍትሔ ታውቃለች። ቦብ እንዲህ ያለ ሙሌት እንዳለ ማመን ይፈልጋል፤ አሊስ ግን መፍትሔውን መግለጥ አትፈልግም። ሙሉ ሙሌት-ውን ከላከች ቦብ ይረጋገጣል፤ ግን ምስጢሩ ይጠፋል።

በክላሲካል ዜሮ-እውቀት ስሪት፣ አሊስ እና ቦብ ይገናኛሉ ያደርጋሉ። አንድ አሮጌ-ዓይነት የአእምሮ ሞዴል የተሸፈኑ ሰቆች ይጠቀማል። አሊስ የተፈታ ፍርግርግ-ውን ትደብቃለች፣ በእያንዳንዱ ዙር በስውር ምልክቶች-ን እንደገና ትሰይማለች፣ እና ቦብ በየዘፈቀደ የተመረጠ አንድ አካባቢያዊ ገደብ — ረድፍ፣ ዓምድ፣ ንዑስ ክፍል ወይም ረዳት አወቃቀር — እንዲመረምር ትፈቅዳለች። የተከፈቱ ሴሎች ሁሉም-የተለያዩ ምልክቶች ካሳዩ፣ ቦብ እምነቱን ይጨምራል። ከዚያ ሁሉም እንደገና ይሸፈናሉ፣ ምልክቶችም አዲስ ስም ያገኛሉ። (አንድ የሚያወሳስብ ነገር፡- የእንቆቅልሹ የተሰጡ ፍንጮች ተጨማሪ ዘዴ ይፈልጋሉ፣ ምክንያቱም እንደገና መሰየም እነሱንም ይደብቃል። ከታች ያለው note ክላሲካል ፕሮቶኮሎች ይህን እንዴት እንደሚፈቱ ይገልጻል፤ ለቀጣዩ ሐሳብ ቀለል ያለ picture-ው በቂ ነው።)

> ### ክላሲካል ፕሮቶኮሎች ፍንጭ ሴሎችን በእውነት እንዴት ይይዛሉ?
>
> እንደገና መሰየም ዘዴ-ው አንድ ያልታየ ችግኝ አለው። ረድፍ፣ ዓምድ እና ንዑስ ክፍል ደንቦች ሁሉ “እነዚህ ሴሎች ሁሉ የተለያዩ ናቸው” ይላሉ፣ ሁሉም የተለያዩ ደግሞ ምልክቶች-ን ምንም እንደገና ብንሰይም ይቀራል። ግን ፍንጭ “ይህ ሴል በትክክል 5 ይይዛል” ይላል፤ ከእንደገና መሰየም በኋላ ቦብ $\sigma(5)$ — አንድ masked ምልክት — ብቻ ያያል፤ እንደገና መሰየም σ-ውን አያውቅም። ምንም ማረጋገጥ አይችልም። ይህ ካልተስተካከለ አሊስ የታተሙ ፍንጮችን በሙሉ ችላ ብላ አንድ valid ፍርግርግ እንዳለ ማረጋገጥ ትችላለች፣ ይህም ስለዚህ እንቆቅልሽ ምንም አያረጋግጥም። ክላሲካል literature ሁለት መደበኛ repairs አሉት።
> **ፓሌት-ው።** በhidden ፍርግርግ ላይ N ሴሎች ያለው አንድ ተጨማሪ ረድፍ ይጨምሩ — አሊስ ምልክቶች 1…Nን በቋሚ public order የምታስቀምጥበት ፓሌት፣ ከዚያም ከሌላው ሁሉ ጋር እንደገና ትሰይመዋለች፣ ስለዚህ $\sigma(1)\ldots\sigma(N)$ ይይዛል። ቦብ የዘፈቀደ ፈተና አሁን አንድ ተጨማሪ option አለው። ረድፍ፣ ዓምድ፣ ንዑስ ክፍል ወይም ረዳት አወቃቀር ከመምረጥ በተጨማሪ ፓሌት-ውን ከአንድ ፍንጭ ሴል ጋር ሊመርጥ ይችላል። አሊስ ሁለቱንም ትከፍታለች፤ ፓሌት-ው የዚያ ዙር እንደገና መሰየም-ን ያሳያል፣ ቦብም ፍንጭ ሴል በትክክል የታተመውን ፍንጭ renamed ስሪት እንደሚያሳይ ይመረምራል። ይህ ዜሮ-እውቀት እንደሆነ ይቀራል፣ ምክንያቱም ቦብ የሚማረው σ ብቻ ነው — በእያንዳንዱ ዙር አዲስ የሚመረጥና ብቻውን ምንም ዋጋ የሌለው — እና ከእንቆቅልሹ ቀድሞውኑ የሚያውቀው ሴል እሴት። ስለምስጢራዊ ሴሎች ምንም አይፈስስም፣ አስመሳይም የዘፈቀደ σ በመምረጥ ይህን እይታ ማስመሰል ይችላል። ትክክል ነው፣ ምክንያቱም cheating አሊስ በእያንዳንዱ ዙር በቋሚ probability ትያዛለች፣ ዙሮችም ጥርጣሬው negligible እስኪሆን ይደገማሉ።
> **ፍንጮችን ከሥርዓቱ ውስጥ compile ማድረግ።** ይበልጥ structural variant ልዩ ፈተና ከመጨመር ይልቅ ያስወግደዋል። ፍንጭ እሴት-ውን መመርመር ሳይሆን difference ገደቦች በመጠቀም ያስገድዱታል፦ ፍንጭ ሴል-ውን የራሱ እሴት ከሚይዘው ፓሌት ሴል በስተቀር ከሁሉም ፓሌት ሴሎች ጋር ያገናኙ — “ከ$\sigma(1)$ የተለየ፣ ከ$\sigma(2)$ የተለየ፣ …፣ ከ$\sigma(5)$ በስተቀር ከሁሉም የተለየ።” ሴል-ው የተፈቀደ ሆኖ ሊይዘው የሚችለው ፍንጭ-ው ብቻ ይሆናል። እያንዳንዱ ገደብ እንደገና “እነዚህ ሁለት የተለያዩ ናቸው” የሚል ዓይነት ይሆናል

> — እንደገና መሰየም ላይ invariant፣ እንደ ረድፍ በትክክል ሊመረመር የሚችል። ይህ በክላሲካል graph-coloring ፕሮቶኮል ውስጥ pre-colored vertices ላይ የሚጠቀሙት ተመሳሳይ ዘዴ ነው፣ እና ከላይ ያለው ረዳት አወቃቀሮች የሚለውም ይህን መንፈስ ይይዛል፡- በሜጋ-ሱዶኩ-as-SAT picture ፍንጮች እንደ ሌሎች ገደቦች ሁሉ ወደ inequality ረዳት አወቃቀሮች ይcompiled ይደረጋሉ።
> **አካላዊ ፕሮቶኮል-ው።** በእውነተኛ ካርዶች የሚሠራው ሱዶኩ ፕሮቶኮል (Gradwohl, Naor, Pinkas and Rothblum, 2007) እንደገና መሰየም ፈጽሞ አይጠቀምም፣ ፍንጮችንም መደበቅ ከመጀመሩ በፊት ይወስናል። ለእያንዳንዱ ሴል አሊስ ተመሳሳይ እሴት ያላቸው ሶስት ተመሳሳይ ካርዶች ታስቀምጣለች — ምስጢራዊ ሴሎች ላይ ፊታቸውን ወደታች፣ ፍንጭ ሴሎች ላይ ግን ፊታቸውን ወደላይ፣ ስለዚህ ቦብ ካርዶች ከመገልበጣቸው በፊት ፍንጮች እንደተከበሩ በዓይኑ ያያል። ከዚያ ከእያንዳንዱ ሴል አንድ ካርድ ወደ ረድፍ ጥቅል፣ አንድ ወደ ዓምድ ጥቅል፣ አንድ ወደ ንዑስ ክፍል ጥቅል ይገባል። እያንዳንዱ ጥቅል ይቀላቀላል፣ ይገለጣል፣ ቦብም ሁሉንም N ምልክቶች እንደያዘ ይመረምራል። መቀላቀል የቦታ መረጃን ያጠፋል — ይህ ዜሮ-እውቀት ነው — ፍንጮች ግን በdealing ጊዜ ቀድሞውኑ ተረጋግጠዋል።
> በሁለቱም መንገድ ትምህርቱ ይህ ጽሑፍ ደጋግሞ ወደሚመለስበት ነጥብ ነው፡- ዜሮ-እውቀት ፕሮቶኮል በመደበቅ ውስጥ የትኞቹ እውነታዎች እንደሚቀሩ ጥንቃቄ ያለው bookkeeping ነው። እንደገና መሰየም “ሁሉም የተለያዩ”ን ይጠብቃል፣ “ከ5 ጋር እኩል”ን ያጠፋል — ስለዚህ “ከ5 ጋር እኩል” በሌላ መንገድ ወደ ውስጥ እንደገና መግባት አለበት።

ይህ በጽሑፉ ውስጥ ያለው ፕሮቶኮል አይደለም። ክላሲካል ዜሮ-እውቀትን ለማሰብ የአእምሮ ሞዴል ነው፡-

- አሊስ እና ቦብ ወደፊት-ወደኋላ ይገናኛሉ።
- ቦብ የዘፈቀደ ፍተሻዎች ይመርጣል።
- አሊስ ሙሉ መፍትሔውን ሳትገልጥ አካባቢያዊ ወጥነት ብቻ ታሳያለች።
- ግላዊነት ማረጋገጫው ቦብ ያየው እይታ የአሊስ ምስጢራዊ መፍትሔ ሳይኖር ሊመነጭ እንደሚችል በማሳየት ይሠራል።

ስለዚህ ክላሲካል ዜሮ-እውቀት በአንድ አዎንታዊ እውነታ ላይ የተገነባ ነው፡-

> አስመሳይ በእውነት አለ።

አሁን ምቹ ክፍሎቹን ያስወግዱ። አሊስ አንድ ማረጋገጫ ሕብረቁምፊ ብቻ ትልካለች እና ትሄዳለች። የታመነ ቅድመ-ዝግጅት የለም፣ አስቀድሞ የተዘጋጀ የጋራ የዘፈቀደ ሕብረቁምፊ የለም፣ ቦብም ሐሰት እንቆቅልሽ ፈጽሞ መቀበል የለበትም። ይህ ክላሲካል ዜሮ-እውቀት መቆየት የማይችልበት ሁኔታ ነው።

ዘዴ-ው ከመግባቱ በፊት አንድ ተጨማሪ ተዋናይ ያስፈልጋል። **የደንብ ሥርዓት ይወስኑ፡-** በlogician ትርጉም መደበኛ የማረጋገጫ ሥርዓት — ቋሚ አክሲዮሞች ስብስብ እና የተጻፉ የሒሳብ ማረጋገጫዎችን ለመመርመር mechanical ደንቦች። ZFC፣ የሒሳብ መደበኛ አክሲዮሞች፣ canonical ምሳሌ ነው። ከዚህ በኋላ ሁሉም ነገር አስቀድሞ ከተመረጠ የደንብ ሥርዓት ጋር አንጻራዊ ሆኖ ይነገራል፣ እና choice-ው flexible ነው፡- ግንባታው ለመረጡት ማንኛውም የደንብ ሥርዓት ይሠራል፣ ZFCን ጨምሮ።

(ከጽሑፉ የተዋሰ የቃላት ማስታወሻ፡- “የማረጋገጫ ሥርዓት” እዚህ ሁልጊዜ ይህን የደንብ ሥርዓት — የሒሳብ ማረጋገጫዎችን የሚመረምር መደበኛ ሥርዓት — ማለት ነው፣ አሊስ የምትልካቸው messages አይደሉም። የአሊስ እና ቦብ አሠራር “ማስረጃ አቅራቢ and አረጋጋጭ” ይባላል።)

የጎደል ዓይነት ስሪት ሜጋ-ሱዶኩ story-ውን ያቆያል፣ ማረጋገጫውን ግን ይቀይራል።

በተመሳሳይ displayed size ያለ ሁለተኛ የገደቦች ሥርዓት ይምረጡ፣ D እንበለው። ለታሪኩ S እና D ተመሳሳይ ቅርጽ ያላቸው ሁለት ሜጋ-ሱዶኩ(n) እንቆቅልሾች ናቸው። በውስጥ ግን D በተለየ size ካለ ከባድ ሎጂካዊ ቀመር ሊጀምር

ይችላል፣ ካስፈለገ በharmless ማሟያ ገደቦች ተጨምሮ ከፍርግርግ-ው ጋር ይስማማል። D በእውነት **ሊሟላ የማይችል** ከሆነ ሎጂካዊ ቀመር ይገነባል፦ ሁሉንም ገደቦች ትክክል የሚያደርግ ምንም ምደባ የለም፣ እንደ የተበላሸ እንቆቅልሽ ምንም የተፈቀደ completed ፍርግርግ የለውም። ቀለል ያለ ምሳሌ “X እውነት ነው” እና “X ሐሰት ነው” ሁለቱንም የሚጠይቅ ቀመር ሊሆን ይችላል። ስለዚህ D ምንም valid ሙሌት የለውም።

ግን D መበላሸቱ **በቀላሉ ሊጋለጥ** የሚችል እንቆቅልሽ መሆን የለበትም። ከላይ ያለው ቀለል ያለ ምሳሌ ይህን አያሟላም፦ ማንኛውም የደንብ ሥርዓት “X and not-X”ን በአንድ መስመር ይማስተባበል ያደርገዋል። D የመረጡት የደንብ ሥርዓት በአጭር argument ሊcertify በማይችለው መንገድ ሐሰት መሆን አለበት። የደንብ ሥርዓቱ Dን በአጭር ማረጋገጫ ሊማስተባበል ቢችል፣ ከታች ያለው ታሪክ ይወድቃል፦ የአሊስ ምስጢር ሳይኖር ምናልባት ማረጋገጫዎች ሊያመነጭ የሚችለው አማራጭ መንገድ በመደበኛ ትርጉም ሊወገድ ይችላል፣ እና ግላዊነት ዋስትናውም አብሮ ይወድቃል። ስለዚህ D ከቋሚ የደንብ ሥርዓት ጋር በብቃት ሊማስተባበል ከማይችሉ ቤተሰብ ይመረጣል፦ በዚያ የደንብ ሥርዓት ውስጥ D መፍትሔ እንደሌለው የሚያሳይ አጭር ማረጋገጫ የለም።

የአሊስ አንድ-መልዕክት ማረጋገጫ ከዚያ ስለ ወይም/or አባባል ይሆናል፦

> ወይም እውነተኛው ሜጋ-ሱዶኩ S መፍትሔ አለው፣ ወይም ማዘናጊያ D መፍትሔ አለው።

ይህ ሎጂካዊ ግንኙነት ነው። D Sን እውነት የሚያደርግ አስማታዊ ነገር አይደለም። ማረጋገጫው “D መፍትሔ የለውም፣ ስለዚህ S መፍትሔ አለው” እያለ አይከራከርም። S or D የወይም አባባል-ን ነው የሚያረጋግጠው። Perfect ትክክለኛነት ሐሰት የወይም አባባል ትክክለኛ ማረጋገጫ ሊኖረው እንደማይችል ይላል። D በእውነት ሐሰት ነው — መፍትሔ የለውም — ስለዚህ የወይም አባባል-ው እውነት ሊሆን የሚችለው S እውነት ከሆነ ብቻ ነው። ማረጋገጫው ከተቀበለ፣ S መፍትሔ መኖሩ አለበት። ማዘናጊያ-ው ሐሰት Sን እውነት ማድረግ አይችልም።

ግን ለዜሮ-እውቀት-ዓይነት ክፍሉ፣ D መፍትሔ ቢኖረው ምን ይሆን ነበር? ብለን እንጠይቅ። ያ ማዘናጊያ መፍትሔ አማራጭ ምስክር ሆኖ ይሠራ ነበር። የአሊስ እውነተኛ ሜጋ-ሱዶኩ መፍትሔ ሳያውቅ ማረጋገጫዎች ማመንጨት ያስችል ነበር — በሌላ ቃል አስመሳይ። በእውነት D መፍትሔ የለውም፣ ስለዚህ ይህ አስመሳይ መንገድ ዝግ ነው። ነጥቡ ግን የደንብ ሥርዓቱ ይህ መንገድ ዝግ መሆኑን በብቃት ማረጋገጥ አለመቻሉ ነው።

ስለዚህ D ሁለት ሥራዎች አሉት። **ለትክክለኛነት** D ሐሰት ነው፣ ስለዚህ “S or D” ትክክለኛ ማረጋገጫ Sን ያስገድዳል። **ለተግባራዊ ዜሮ-እውቀት** D ለማስተባበያ ከባድ ነው፣ ስለዚህ የደንብ ሥርዓቱ ማስመሰልን ሊያስችል የነበረውን ማዘናጊያ መንገድ በፍጥነት ማስወገድ አይችልም።

ስለዚህ የደህንነት ፈተና-ው ከእንግዲህ፦

> አስመሳይ በእውነት እንዳለ ማረጋገጥ እንችላለን?

አይደለም። ወደዚህ ይቀየራል፦

> የደንብ ሥርዓት-ዎ አስመሳይ የማይቻል መሆኑን በብቃት ማረጋገጥ ይችላል?

መልሱ “አይ” ከሆነ፣ አስገራሚ ጠንካራ ነገር ይከተላል፦ እያንዳንዱ የደህንነት ዋስትና (a) በሙከራ በማስኬድ ሊታይ የሚችል እና (b) በዚያ የደንብ ሥርዓት ውስጥ አስመሳይ መኖሩ እንዲያመጣው በማረጋገጫ የተረጋገጠ ከሆነ፣ በእውነት ይሠራል። በእነዚህ ማንኛውም ላይ የተሳካ ጥቃት መኖሩ ራሱ የጎደለው አጭር ማስተባበያ ይሆን ነበር፣ ያ አጭር ማስተባበያ ግን የለም። ይህ የ“effectively” ዜሮ-እውቀት ተግባራዊ ክፍል ነው።

ስለዚህ ለመማሪያ የሚሆን ንጽጽር-ው፦

ክላሲካል ዜሮ-እውቀት፡- ማረጋገጫዎች ደህና ናቸው ምክንያቱም አስመሳይ አለ።

የጎደል ዓይነት ተግባራዊ ዜሮ-እውቀት፡- ለሊታዩ የደህንነት ፈተናዎች ማረጋገጫዎች ደህና እንደሆኑ ይወሰዳሉ፣ ምክንያቱም የደንብ ሥርዓቱ አስመሳይ የማይቻል መሆኑን በብቃት ማረጋገጥ አይችልም።

ሁለተኛው አባባል ደካማ ነው። ግን ይህ ደካማነት ነው ጽሑፉ በክላሲካል ስሪት የተሰበሩትን ሶስት ባህሪያት — አንድ መልዕክት፣ ቅድመ-ዝግጅት የለም፣ ፍጹም ትክክለኛነት — ማቆየት የሚችለው።

አዲሱ ፈተና፡- አስመሳይ እንደሌለ ማረጋገጥ አይቻልም

የIlango ማላላት ጥያቄውን ይቀይራል።

ክላሲካል ዜሮ-እውቀት፡-

> አስመሳይ አለ?

ይጠይቃል።

በተግባር ዜሮ-እውቀት ይበልጥ ደካማ ጥያቄ ይጠይቃል፡-

> የመረጡት የደንብ ሥርዓት አስመሳይ የለም ብሎ በብቃት ማረጋገጥ ይችላል?

ይህ ቴክኒካዊ መሸሻ ሊመስል ይችላል፣ ግን ዋናው ሐሳብ ነው። ግንባታው እንግዳ ሁኔታ ውስጥ ይኖራል፡- አስመሳይ በእውነት የለም — ጽሑፉ በግልጽ ይላል — ግን እርስዎ የመረጡት የደንብ ሥርዓት አስመሳይ እንደሌለ በብቃት ማረጋገጥ አይችልም። እርስዎ የምትጨነቁባቸው ሁሉም አሉታዊ መዘዞች እንዲህ ያለ ማስተባበያ የሚፈልጉ ከሆኑ፣ ሥርዓቱ ለእነዚያ መዘዞች እንደ ዜሮ-እውቀት ይሠራል።

ጎደል የሚገባው እዚህ ነው። እንደ ማስዋብ አይደለም፣ "ጎደል ክሪፕቶግራፊ-ን ደህና ያደርገዋል" ማለትም አይደለም። Connection-ው ማረጋገጫ-ንድፈ-ሐሳባዊ ነው። የደንብ ሥርዓት ምርጥ የሚባለው፣ በትክክለኛ ትርጉም ምርጥ የሚቻለው ከሆነ ነው፡- ማንኛውም የደንብ ሥርዓት ተገቢውን ቀመር በአጭር ማረጋገጫ ሊማስተባበል ሲችል፣ ምርጥ የደንብ ሥርዓቱም ሊማስተባበል ይችላል፣ ማረጋገጫውም ቢበዛ በፖሊኖሚያል መጠን ብቻ የሚረዝም ይሆናል። Krajíček እና Pudlák በ1989 **ምንም ምርጥ የማረጋገጫ ሥርዓት የለም** የሚል ግምት አቀረቡ፡- ማንኛውንም የደንብ ሥርዓት ቢያስቀምጡ፣ አንድ ሌላ የደንብ ሥርዓት አንዳንድ የእውነት አባባሎች ቤተሰብን በጣም አጭር ማረጋገጫዎች ያረጋግጣል። ይህ ከየማረጋገጫ ውስብስብነት ዋና ያልተፈታ ግምቶች አንዱ ነው፣ እና ጎደል አለመሟላት ቲዎረም ውሱን፣ የውስብስብነት ንድፈ-ሐሳብ ዘመድ ነው፡- አንዳንድ እውነት አባባሎች በመረጡት የደንብ ሥርዓት ውስጥ አጭር ማረጋገጫ የላቸውም — በመሠረቱ ሊማረጋገጥ ስለማይችሉ አይደለም፣ ግን እያንዳንዱ ቋሚ የደንብ ሥርዓት አንዳንድ አጭር truthsን ያለ አጭር ማረጋገጫዎች ስለሚተው።

ጽሑፉ ይህን ግምት (በትንሽ የበለጠ ጠንካራ "infinitely often" form፣ conjectures በክሪፕቶግራፊ ሲጠቀሙ የተለመደ) እንደ ግምት ይወስዳል። ከKrajíček እና Pudlák ቲዎረም የሚመጣው payoff ግልጽ ነው፡- ለእያንዳንዱ የደንብ ሥርዓት በእውነት ሊሟላ የማይችል የሆኑ፣ ግን የደንብ ሥርዓቱ በአጭር ማረጋገጫዎች ሊማስተባበል የማይችላቸው ቀመሮች ተከታታይ አለ፣ እና በጣም አስፈላጊው፣ ውጤታማ አልጎሪዝም እነሱን **ማመንጨት** ይችላል። ይህ የuniformity ባህሪ ሐሳቡን ከexistence አባባል ወደ አሊስ በእውነት ልታስኬደው ወደምትችል አልጎሪዝም ይቀይረዋል፡- ማዘናጊያዎች D ከassembly መስመር ይወጣሉ፣ ከባዶ አይመጡም።

የክሪፕቶግራፊ እርምጃ-ው ያ ማረጋገጫ የማረጋገጫ አቅም እጥረት ለደህንነት መጠቀም ነው።

ግንባታው ምን እየሠራ ነው?

የጽሑፉ ግንባታ በንጹህ ቅርጽ እንዲህ ነው።

የደንብ ሥርዓት ይወስኑ — ለምሳሌ ZFC። በማረጋገጫ-ውስብስብነት ግምት ስር፣ በብቃት ሊፈጠር የሚችሉ፣ በእውነት ሊሟላ የማይችል የሆኑ፣ ግን የደንብ ሥርዓቱ ሊሟላ የማይችል መሆናቸውን የሚያሳይ አጭር ማረጋገጫ የሌለው ቀመሮች ተከታታይ አለ።

አሁን እንዲህ ያለ አንድ-መልዕክት ማረጋገጫ ይገንቡ:-

> ወይም እውነተኛው አባባል ሊሟላ የሚችል ነው፣ ወይም ይህ ልዩ ከባድ ቀመር ሊሟላ የሚችል ነው።

ልዩ ከባድ ቀመሩ ሊሟላ የሚችል አይደለም። ስለዚህ underlying ማረጋገጫ አሠራር ፍጹም ትክክል ከሆነ፣ መልዕክቱን መቀበል አሁንም እውነተኛ አባባሉ እውነት መሆኑን ያመለክታል። ይህ ፍጹም ትክክለኛነት ይሰጣል።

ግን ለዜሮ-እውቀት-like ደህንነት፣ ልዩ ከባድ ቀመሩ ሊሟላ የሚችል ቢሆን ብለው ያስቡ። ምስክሩ እውነተኛ ምስክሩን ሳያውቅ ማረጋገጫዎች ለsimulate ማድረግ ሊጠቀም ይችል ነበር። ቀመሩ በእውነት ሊሟላ የሚችል አይደለም — ግን የደንብ ሥርዓቱ ይህን በብቃት ማረጋገጥ አይችልም። ስለዚህ አስመሳይ የማይቻል መሆኑን በብቃት ማረጋገጥ አይችልም።

ዋና hinge-ው ይህ ነው። ሥርዓቱ ምስጢሩን ክላሲካል አስመሳይ በማመንጨት አይደብቅም። ለትልቅ ክፍል ሊታዩ የሚችሉ የደህንነት ፈተናዎች፣ አስመሳይ እንደሌለ ማረጋገጥ የደንብ ሥርዓቱ አለመቻል ጀርባ ላይ ያስቀምጠዋል።

ጽሑፉ ምን አባባል ያደርጋል?

ዋና ቲዎረም በlayers ይመጣል። ዋና ውጤት ይህ ነው:-

በመደበኛ ክሪፕቶግራፊያዊ ግምት — መስተጋብር-አልባ ምስክር ሊለዩ የማይችሉ ማረጋገጫዎች መኖር፣ በደንብ የተጠኑ ነገሮች እና ከብዙ የተመሰረቱ ግምት ስብስቦች የሚከተሉ — እና no (infinitely often) ምርጥ የማረጋገጫ ሥርዓት አለ በሚለው ማረጋገጫ-ውስብስብነት ግምት ስር፣ ጽሑፉ ለእያንዳንዱ የደንብ ሥርዓት አንድ-መልዕክት ማስረጃ አቅራቢ እና አረጋጋጭ ለNP/SAT ይገነባል፤ ፍጹም ትክክለኛነት እና ቅድመ-ዝግጅት የለም ያለው፣ ከዚያ የደንብ ሥርዓት ጋር አንጻራዊ ሆኖ በተግባር ዜሮ-እውቀት የሆነ። (NP/SAT የእንቆቅልሽ-like ችግሮች መደበኛ "hardest የተለመደ denominator" ነው፤ ሜጋ-ሱዶኩ ከሚለብሳቸው ልብሶች አንዱ ብቻ ነው።)

ሊስተባበል የሚችል የደህንነት ባህሪያትን በሰፊው ለማቆየት የሚለው ሰፋ ያለ አባባል አንድ ተጨማሪ መደበኛ ግምት ይጨምራል:- የዘፈቀደነትን የማስወገድ ግምት P = BPP (በግምት:- የዘፈቀደነት አልጎሪዝሞችን ከመሠረታዊ ተጨማሪ ኃይል አያገኙላቸውም)።

ቲዎረም ቋንቋን ካስወገድን:-

- ማረጋገጫው አንድ መልዕክት ነው።
- የታመነ ቅድመ-ዝግጅት የለም።
- ሐሰት አባባሎች ሊproved አይችሉም።
- ማስረጃ አቅራቢው ክላሲካል ዜሮ-እውቀት አይደለም — አስመሳይ የለውም።
- ግን እያንዳንዱ ሊስተባበል የሚችል፣ በጨዋታ ሙከራ ላይ የተመሠረተ ደህንነት መዘዝ of ክላሲካል ዜሮ-እውቀት በዚህ አውድ ሊገኝ ይችላል።

“ሊስተባበል የሚችል” አስፈላጊ ነው። ደህንነት ውድቀት በጨዋታ ውስጥ ተቃዋሚ በማስኬድ ሊፈተን ይችላል ማለት ነው። ብዙ ክሪፕቶግራፊያዊ የደህንነት ትርጉሞች እንዲህ ያለ ቅርጽ አላቸው:- ተቃዋሚ ሁለት encryptionsን ሊለይ ይችላል? Functionን invert ማድረግ ይችላል? ምስክርን recover ማድረግ ይችላል? ወይስ በተወሰነ ሙከራ ማሸነፍ ይችላል? ቲዎረም-ው ለእያንዳንዱ ሊስተባበል የሚችል ባህሪ፣ አንድ በአንድ፣ ማስረጃ አቅራቢ ይሰጣል። አንድ ማስረጃ አቅራቢ ሁሉንም ሊስተባበል የሚችል ባህሪያት በአንድ ጊዜ እንዲያሟላ ማድረግ ምናልባት አይቻልም — አሮጌው ዳግም-መጠቀም ጥቃት (“ቦብ ማረጋገጫውን ለሌሎች ማሳየት ይችላል”) ራሱ ሊስተባበል የሚችል ባህሪ ነው፣ እና እዚህ በእውነት ይወድቃል። ጽሑፉ አንድ ማስረጃ አቅራቢ ሁሉንም ተፈጥሯዊ ሊስተባበል የሚችል ባህሪያት — በየክሪፕቶግራፊ ተግባር በእውነት የሚገኙትን — ሊሸፍን ይችላል ብሎ ይጠቁማል፣ ግን ይህ ክፍል መደበኛ ያልሆነ “ተፈጥሯዊ” ትርጉም እና ግልጽ ግምት ላይ የተመሠረተ በሁኔታ የተገደበ ቲዎረም ነው። ዋስትና-ው ወደ ሊታይ የሚችል ውድቀቶች ይመለከታል፣ ሁሉንም ፍልስፍናዊ ወይም በማስመሰል ላይ የተመሠረተ የምስጢራዊነት ትርጉሞች አይሸፍንም።

አንድ ተጨባጭ ተከታይ ውጤት ስም ሊጠቀስ ይገባዋል:- ግንባታው በወጥ ማስረጃ አቅራቢ የመጀመሪያ መስተጋብር-አልባ ምስክር መደበቅ ማረጋገጫዎች ይሰጣል — “የእንቆቅልሽ ማረጋገጫ መኖሩ መፍትሔውን ለማግኘት አይረዳዎትም”፣ መስተጋብር ወይም ቅድመ-ዝግጅት የለም — ቀላል የሚመስል ግን ለአስርተ ዓመታት ግንባታውን የተቋቋመ ነገር።

ይህ ምን አይልም?

ይህ ክፍል ጽሑፉን ጥንቃቄ ያለው ያደርገዋል።

አሮጌ የማይቻልነት ቲዎረሞች ስህተት ነበሩ ብሎ አይልም። ግንባታው ትርጉም-ውን በመቀየር ነው የሚያልፋቸው።

No መስተጋብር፣ ቅድመ-ዝግጅት የለም እና ፍጹም ትክክለኛነት ያለው መደበኛ ክላሲካል ዜሮ-እውቀት አይሰጥም። ጽሑፉ constructed ማስረጃ አቅራቢ አስመሳይ እንደሌለው በግልጽ ይላል።

ማረጋገጫው እንደገና ሊጠቀም አይችልም ማለት አይደለም። One-መልዕክት ማረጋገጫ አሁንም ለሌላ ሰው ሊታይ ይችላል፤ ጽሑፉ deniability-ዓይነት ባህሪያትን አያቀይም። (የታመነ ቅድመ-ዝግጅት ያለው መስተጋብር-አልባ ዜሮ-እውቀት እንኳን ተመሳሳይ ገደብ አለው።)

ይህ ለተግባራዊ ማሰማራት ዝግጁ የሆነ ተግባራዊ ፕሮቶኮል ነው ማለት አይደለም። ይህ ውስብስብነት ንድፈ ሐሳብ እና ክሪፕቶግራፊያዊ foundations ነው። ውጤት-ው ከየማረጋገጫ ውስብስብነት እና ክሪፕቶግራፊ ትልቅ ግምቶች ላይ ይመሰረታል፣ ግንባታውም በprinciple ምን ሊቻል እንደሚችል ነው።

“ጎደል” አስማታዊ ደህንነት መሠረታዊ መሣሪያ ነው ማለት አይደለም። ጎደል connection-ው በየማረጋገጫ ሥርዓቶች፣ ምርጥ የማረጋገጫ ሥርዓቶች እና ውሱን analogues of አለመሟላት በኩል ነው። ጠቃሚ ግንዛቤ “አለመሟላት password-ዎን ይጠብቃል” አይደለም። ይህ ነው:- የደንብ ሥርዓት አንድ አስመሳይ የማይቻል መሆኑን በብቃት ማረጋገጥ ካልቻለ፣ ያንን ማረጋገጫ የሚፈልጉ ጥቃቶች በየደህንነት ትርጉሞች ደረጃ ሊታገዱ ይችላሉ።

ቢሆንም ለምን አስደሳች ነው?

ክሪፕቶግራፊ ብዙ ጊዜ አስቸጋሪነትን ወደ ደህንነት ይቀይራል። Factoring ከባድ ነው፣ ስለዚህ RSA-ዓይነት ግምቶች ጠቃሚ ይሆናሉ። Lattice ችግሮች ከባድ ናቸው፣ ስለዚህ lattice ክሪፕቶግራፊ ጠቃሚ ይሆናል። እዚህ አስቸጋሪነት-ው ይበልጥ እንግዳ ነው:- “ምስጢር ለማስላት ከባድ” አይደለም፣ “የተወሰነ ማረጋገጫ ነገር ሊኖር አይችልም ብሎ ማረጋገጥ

ከባድ” ነው።

ጽሑፉ ያልተለመደ የሚመስለው ለዚህ ነው። አክሲዮሞች እና rulebooksን እንደ የክሪፕቶግራፊ ሀብቶች በሚመስል መንገድ ይይዛል። መደበኛ የማይቻልነት በትክክለኛነት እና ማስመሰል መካከል tension አለ ይላል። የIlango move ያ tension-ን ከማረጋገጫ-ንድፈ-ሐሳባዊ curtain ጀርባ ያስቀምጣል፦ አስመሳይ የለም፤ ግን መደበኛ ሥርዓቱ ይህን አለመኖር በብቃት ማጋለጥ አይችልም።

ለአንባቢ አስገራሚው ነገር ይህ የዛሬ ዜሮ-እውቀት ሥርዓቶቹን ይተካል የሚለው አይደለም። ቢያንስ በቀጥታ ምናልባት አይተካቸውም። አስገራሚው ነገር ከmathematical logic የመጣ ገደብ በconstructive መንገድ ሊጠቀም መቻሉ ነው፦ እንደ ግድግዳ ብቻ አይደለም፤ እንደ መሸፈኛም ይሠራል።

ማስረጃው ምን ያህል ጠንካራ ነው?

ይህ ቲዎረም ጽሑፍ ነው፤ ስለዚህ “ማስረጃ” ከbiology ወይም astronomy ጽሑፍ የተለየ ትርጉም አለው። ጥያቄው ሙከራ ተደግሟል ወይ? አይደለም። ትርጉሞች፣ ግምቶች እና ማረጋገጫ chain አባባል-ውን ይደግፋሉ ወይ? ነው።

ማረጋገጫው መደበኛ ነው፤ ጽሑፉም ግምቶች-ዎቹን በግልጽ ያቀርባል። ግምቶች-ዎቹ casual አይደሉም። Non-interactive ምስክር ሊለዩ የማይችሉ ማረጋገጫዎች በክሪፕቶግራፊ የተለመዱ ነገሮች ናቸው እና ከብዙ የተመሰረቱ ግምት ስብስቦች ይከተላሉ። No-ምርጥ-ማረጋገጫ-ሥርዓት ግምት በየማረጋገጫ ውስብስብነት ዋና ግምት ነው። P = BPP ደግሞ ለሰፋ ያለ ሊስተባበል የሚችል-ባህሪ ቲዎረም ብቻ የሚጠቀሙበት መደበኛ የዘፈቀደነትን የማስወገድ ግምት ነው።

ጽሑፉ ግምቶች የተመረጡት በዘፈቀደ እንዳልሆነም ይከራከራል፦ converse ይማረጋገጥ ያደርጋል፤ እነሱ በመሠረቱ አስፈላጊ እንደሆኑ ያሳያል — እንዲህ ያሉ constructions ፈጽሞ ካሉ፣ መስተጋብር-አልባ ምስክር ሊለዩ የማይችሉ ማረጋገጫዎች መኖር አለባቸው፤ እና መደበኛ አንድ-አቅጣጫ ፋንክሽኖችን ካስቀመጥን no ምርጥ የማረጋገጫ ሥርዓት መኖሩ አይቻልም። ግምቶች-ዎቹ “win-win” ናቸው፦ ማንኛውንም መስበር በየማረጋገጫ ውስብስብነት፣ ክሪፕቶግራፊ ወይም ውስብስብነት ንድፈ ሐሳብ ውስጥ ራሱ ታላቅ discovery ይሆናል።

ግን ውጤት-ው በሁኔታ የተገደበ ስለሆነ፣ confidence-ውም በሁኔታ የተገደበ ነው። ግምቶች-ዎቹ ካልሠሩ ቲዎረም-ው የሚተረጎምበት መንገድ ይቀየራል። እና ግምቶች-ዎቹ ትክክል ቢሆኑም ዋስትናው ሙሉ ክላሲካል ዜሮ-እውቀት አይደለም፤ የጽሑፉ relaxed፣ ማረጋገጫ-ንድፈ-ሐሳባዊ ስሪት ነው።

ስለዚህ ትክክለኛው confidence፦ ጽሑፉ coherent በሁኔታ የተገደበ possibility ውጤት እንደሚያቋቁም ላይ ከፍተኛ፤ ግምቶች-ዎቹ እኛ በእውነት የምንኖርበትን የክሪፕቶግራፊ ዓለም እንደሚገልጹ ላይ መጠነኛ፤ ለፈጣን ተግባራዊ መዘዝ ዝቅተኛ።

ለምን አስፈላጊ ነው?

ጽሑፉ ዝግ ነው ተብሎ የታሰበ መንገድ ይከፍታል።

ክላሲካል ንድፈ ሐሳብ፦ ሙሉ ዜሮ-እውቀት ቅድመ-ዝግጅት ሳይኖር አንድ መልዕክት ሊሆን አይችልም፤ ፍጹም ትክክለኛነትም ሊኖረው አይችልም ይላል። የIlango ጽሑፍ ግን እንዲህ ይላል፦ በደህንነት ጨዋታዎች ውስጥ ሊፈተኑ የሚችሉ የዜሮ-እውቀት መዘዞችን ብንጠይቅ፣ እና የደህንነት ትርጉም-ው የደንብ ሥርዓት ምን በብቃት ሊማስተባበል

ወይም ሊያልችል እንደሚችል አንጻራዊ እንዲሆን ብንፈቅድ፣ ብዙ ጠቃሚ ባህሪ እንደገና ማግኘት ይቻላል — በአንድ መልዕክት፣ ቅድመ-ዝግጅት የለም እና ፍጹም ትክክለኛነት።

ይህ ትንሽ definitional tweak አይደለም። ክሪፕቶግራፊያዊ guaranteesን ለማሰብ የተለየ መንገድ ነው። ምን እንዳለ ብቻ ከመጠየቅ ይልቅ፣ የደንብ ሥርዓት-ዎ ምን ማስወገድ እንደሚችል ይጠይቁ። Unprovabilityን እንደ ፍልስፍናዊ nuisance ብቻ ከማየት ይልቅ እንደ structure ይጠቀሙበት።

ተግባራዊ ዓለም ነገ ላይቀየር ይችላል። ግን conceptual map-ው ይቀየራል። አሁን "ምስጢሩ እንደፈሰሰ ማንም በብቃት ማረጋገጥ አይችልም" የሚለው "ምስጢሩ አልፈሰሰም" ከሚለው ለምንፈልጋቸው ብዙ በጨዋታ ሙከራ ላይ የተመሠረተ protections እንደገና ለማግኘት በቂ ጠንካራ ሊሆን የሚችልበት መደበኛ ትርጉም አለ።

ለዚህ ነው ጎደል በርዕስ ውስጥ የሚገባው።

ንጹህ ማጠቃለያ

ዜሮ-እውቀት ማረጋገጫዎች ማስረጃ አቅራቢ አንድ አባባል እውነት መሆኑን ምስክሩን ሳይገልጥ አረጋጋጭን እንዲያሳምን ያስችላሉ። ክላሲካል የማይቻልነት ውጤቶች ዜሮ-እውቀት ቅድመ-ዝግጅት ሳይኖር ወደ አንድ መልዕክት ሊጨመቅ እንደማይችል እና ፍጹም ትክክለኛነት ሊኖረው እንደማይችል ይላሉ። የRahul Ilango ጽሑፍ እነዚህን የማይቻልነት ውጤቶች አያስተባብልም። በተግባር ዜሮ-እውቀት የሚባል ደካማ notion ይገልጻል፡- አስመሳይ በእውነት እንዲኖር ከመጠየቅ ይልቅ፣ እንደ ZFC ያለ የተመረጠ መደበኛ የማረጋገጫ ሥርዓት አስመሳይ እንደሌለ በብቃት ማረጋገጥ እንዳይችል ይጠይቃል። ከክሪፕቶግራፊ የመጡ ትልቅ ግምቶች (መስተጋብር-አልባ ምስክር ሊለዩ የማይችሉ ማረጋገጫዎች) እና ከየማረጋገጫ ውስብስብነት የመጣ ግምት (no ምርጥ የማረጋገጫ ሥርዓት አለ) ስር፣ ጽሑፉ ቅድመ-ዝግጅት የለም እና ፍጹም ትክክለኛነት ያላቸው አንድ-መልዕክት ማስረጃ አቅራቢዎች ለNP/SAT ይገነባል፣ እና የዜሮ-እውቀት ሊስተባበል የሚችል፣ በጨዋታ ሙከራ ላይ የተመሠረተ መዘዞችን ባህሪ በባህሪ ያገኛል። አንድ ማስረጃ አቅራቢ ሁሉንም "ተፈጥሯዊ" የዚህ ዓይነት ባህሪያት እንዲሸፍን የሚለው ተጨማሪ፣ በከፊል በግምት ላይ የተመሠረተ extension ነው — በliteral ትርጉም ሁሉንም ሊስተባበል የሚችል ባህሪያት መሸፈን ምናልባት አይቻልም፣ ምክንያቱም ማረጋገጫዎች አሁንም reusable ናቸው። ውጤት-ው ንድፈ-ሐሳባዊ እና በሁኔታ የተገደበ ነው፣ deployed መሠረታዊ መሣሪያ አይደለም፣ ግን ማረጋገጫ-ንድፈ-ሐሳባዊ unprovabilityን እንደ ክሪፕቶግራፊያዊ resource ለመጠቀም አዲስ መንገድ ያሳያል።

ያለ ማጋነን ፍተሻ

ወረቀቱ የሚያሳየው፡- በተገለጹ ግምቶች ስር፣ ለNP/SAT አንድ-መልዕክት፣ no-ቅድመ-ዝግጅት፣ ፍጹም ትክክል ማስረጃ አቅራቢዎች መገንባት ይቻላል፣ እነሱም ከማንኛውም የተመረጠ የማረጋገጫ ሥርዓት ጋር አንጻራዊ ሆነው በተግባር ዜሮ-እውቀት ናቸው፣ እና እያንዳንዱ ሊስተባበል የሚችል በጨዋታ ሙከራ ላይ የተመሠረተ መዘዝ of ክላሲካል ዜሮ-እውቀት ሊያሟሉ ይችላሉ።

ምክንያታዊ ግን unconditional ያልተረጋገጠው፡- የሚፈለጉት ማረጋገጫ-ውስብስብነት እና ክሪፕቶግራፊያዊ ግምቶች ትክክል መሆናቸው። እነሱ serious፣ well-studied ግምቶች ናቸው — ጽሑፉም በመሠረቱ አስፈላጊ እንደሆኑ እንዲሁም sufficient እንደሆኑ ያሳያል — ግን አሁንም ግምቶች ናቸው።

የማያሳየው፡- no መስተጋብር፣ ቅድመ-ዝግጅት የለም እና ፍጹም ትክክለኛነት ያለው ክላሲካል ዜሮ-እውቀት፣ ለተግባራዊ ማሰማራት ዝግጁ ተግባራዊ ሥርዓት፣ deniability ወይም ማረጋገጫዎች non-ዳግም-መጠቀም፣ ወይም ጎደል አለመሟላት ቲዎረም ብቻውን ክሪፕቶግራፊን ደህና እንደሚያደርግ።

ዋና ገደቦች፡- ዋስትናው የዜሮ-እውቀት ማላላት ነው፤ broadest ስሪት በብዙ ግምቶች ላይ ይመሰረታል፤ single-universal-ማስረጃ አቅራቢ አባባሎች በከፊል በግምት ላይ የተመሠረተ ናቸው፤ እና ውጤት-ው በዋናነት foundational ነው።

አጠቃላይ አንባቢ ምን ያህል እምነት ሊኖረው ይገባል? ትርጉሞች-ዎቹ ከተቀበሉ፣ ይህ አስፈላጊ በሁኔታ የተገደበ ንድፈ ሐሳብ ውጤት መሆኑ ላይ ከፍተኛ እምነት። ግምቶች-ዎቹ realityን እንደሚወክሉ ላይ መጠነኛ እምነት። ለፈጣን ተግባራዊ ተግባራዊ ማሰማራት ዝቅተኛ እምነት። Safe takeaway፡- ጽሑፉ ዜሮ-እውቀት የማይቻልነት ውጤቶችን አይሰብርም፤ ለብዙ ደህንነት ጨዋታዎች አስፈላጊ የሆኑትን ክፍሎች ለማለፍ አዲስ ማረጋገጫ-ንድፈ-ሐሳባዊ መንገድ ያገኛል።

ምንጮች

Ilango, IACR ePrint 2025/1296
https://eprint.iacr.org/2025/1296

FOCS 2025, DOI 10.1109/FOCS63196.2025.00058
https://doi.org/10.1109/FOCS63196.2025.00058