The Clean Paper

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

კრიპტოგრაფიულ მტკიცებულებას საიდუმლოს დაფარვა შეუძლია, თუ სიმულატორის არარსებობის დამტკიცება რთულია

Zero-knowledge proofs საშუალებას იძლევა განცხადება witness-ის გამჟღავნების გარეშე დამტკიცდეს. კლასიკური თეორია ამბობს, რომ სრული მნიშვნელობით ამის ერთ შეტყობინებაში, სანდო setup-ის გარეშე და perfect soundness-ით მიღება შეუძლებელია. რაჰულ ილანგოს ნაშრომი ამ შეუძლებლობას არ აუქმებს; ის მიზანს ცვლის. რეალური სიმულატორის არსებობის ნაცვლად მოითხოვება, რომ არჩეულ proof system-ს არ შეეძლოს ეფექტურად დაამტკიცოს სიმულატორის არარსებობა. Proof complexity-ისა და კრიპტოგრაფიის მნიშვნელოვან დაშვებებზე დაყრდნობით, ეს საკმარისია zero-knowledge-ის falsifiable, game-based შედეგების თითო თვისების მიხედვით აღსადგენად. ეს ინტერნეტში დასანერგი მზა primitive არაა; ეს არის proof-theoretic გზა, რომელიც მათემატიკურ დაუმტკიცებლობას კრიპტოგრაფიულ საფარად იყენებს.

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

ხრიკი ის კი არ არის, დაამტკიცო, რომ საიდუმლო დამალულია

დავიწყოთ ნულოვანი ცოდნის ყველაზე მარტივი ვერსიით.

ალისს სურს ბობი დაარწმუნოს, რომ სუდოკუს ამოცანას ამოხსნა აქვს. თუ ის ამოხსნას გაუგზავნის, ბობი დარწმუნდება — მაგრამ თავსატეხიც გაფუჭდება. ალისს უფრო უცნაური რამ უნდა: დაამტკიცოს, რომ ამოხსნა არსებობს ისე, რომ თავად ამოხსნა არ გაამჟღავნოს.

სწორედ ამას გვპირდება **ნულოვანი ცოდნის მტკიცებულება**. დამმტკიცებელი — ალისი — შემმოწმებელს, ბობს, არწმუნებს, რომ განცხადება ჭეშმარიტია ისე, რომ განცხადების ჭეშმარიტების გარდა არაფერს უმხელს.

პრობლემა ისაა, რომ ამ დაპირებას ფასი აქვს. ჩვეულებრივ მათემატიკურ მტკიცებულებას ორი კომფორტული თვისება გააჩნია. ის **ერთი შეტყობინებაა**: წერ, გადასცემ და მიდიხარ. და ის **სრულყოფილად სანდოა**: მცდარ განცხადებას საერთოდ არ აქვს ვალიდური მტკიცებულება. კლასიკური შეუძლებლობის შედეგები გვეუბნება, რომ ნულოვანმა ცოდნამ ორივე თვისება უნდა დათმოს — და არა მხოლოდ ორივე ერთად; ცალ-ცალკეც თითოეული მიუღწეველია.

პირველი: ნულოვანი ცოდნის მტკიცებულებას დიალოგი სჭირდება. თუ ალისი მხოლოდ ერთ შეტყობინებას აგზავნის და წინასწარ არ არსებობს სანდო მოსამზადებელი გარემო, ნულოვანი ცოდნის გარანტია იშლება — იმის მიუხედავად, რამდენად მზად ვართ სისწორის ალბათობრივი გარანტია დავასუსტოთ.

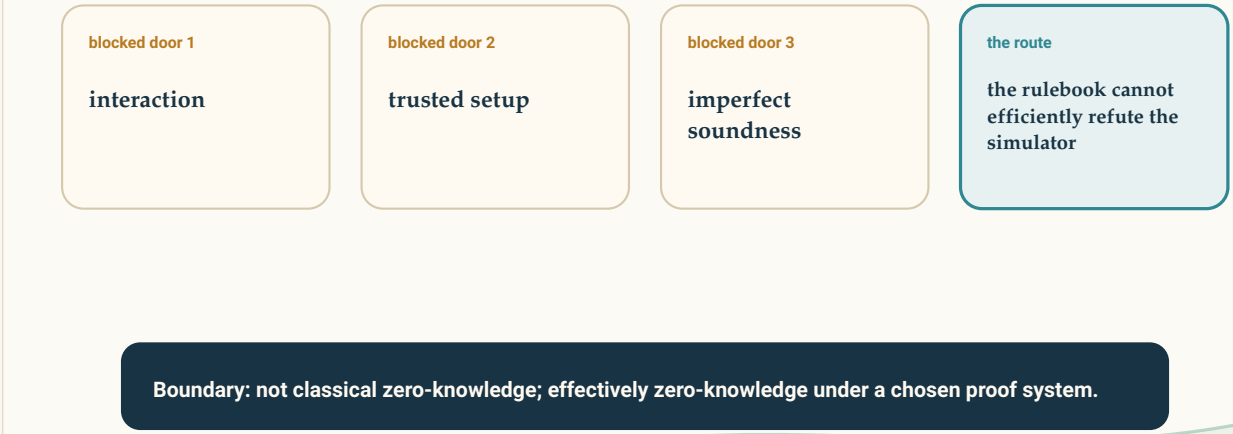
მეორე: ნულოვანი ცოდნის მტკიცებულებას შეცდომის მცირე ალბათობის ატანა სჭირდება. სრულყოფილი სისწორის მოთხოვნა, როგორც აღმოჩნდა, ჩუმად ანადგურებს ინტერაქციასაც: თუ შემმოწმებლის მოტყუება მისი შემთხვევითი არჩევანების მიუხედავად შეუძლებელია, მას შეუძლია ეს არჩევანები წინასწარ დააფიქსიროს; როგორც კი შემმოწმებელი წინასწარ პროგნოზირებადი ხდება, ალისს ყველა პასუხის ერთ შეტყობინებაში ჩატევა შეუძლია — ზუსტად იმ შემთხვევამდე მივდივართ, რომელიც უკვე შეუძლებელი იყო.

რაჰულ ილანგოს ნაშრომი ამ ორმაგი კედლის შემოვლის გზაზეა. არა იმით, რომ კედელი თითქოს არ არსებობს, და არც კლასიკური ნულოვანი ცოდნის მიღებით იმ გარემოში, სადაც ეს შეუძლებელია. ნაბიჯი უფრო დახვეწილია: შესუსტდეს მნიშვნელობა იმისა, რას ნიშნავს „არაფერს ამჟღავნებს“, მაგრამ ისე, რომ შენარჩუნდეს უსაფრთხოების ის თვისებები, რომელთა რეალურად შემოწმებაც კრიპტოგრაფებს შეუძლიათ.

შედეგს ეწოდება **ეფექტური ნულოვანი ცოდნა**.

A proof without leaking the witness

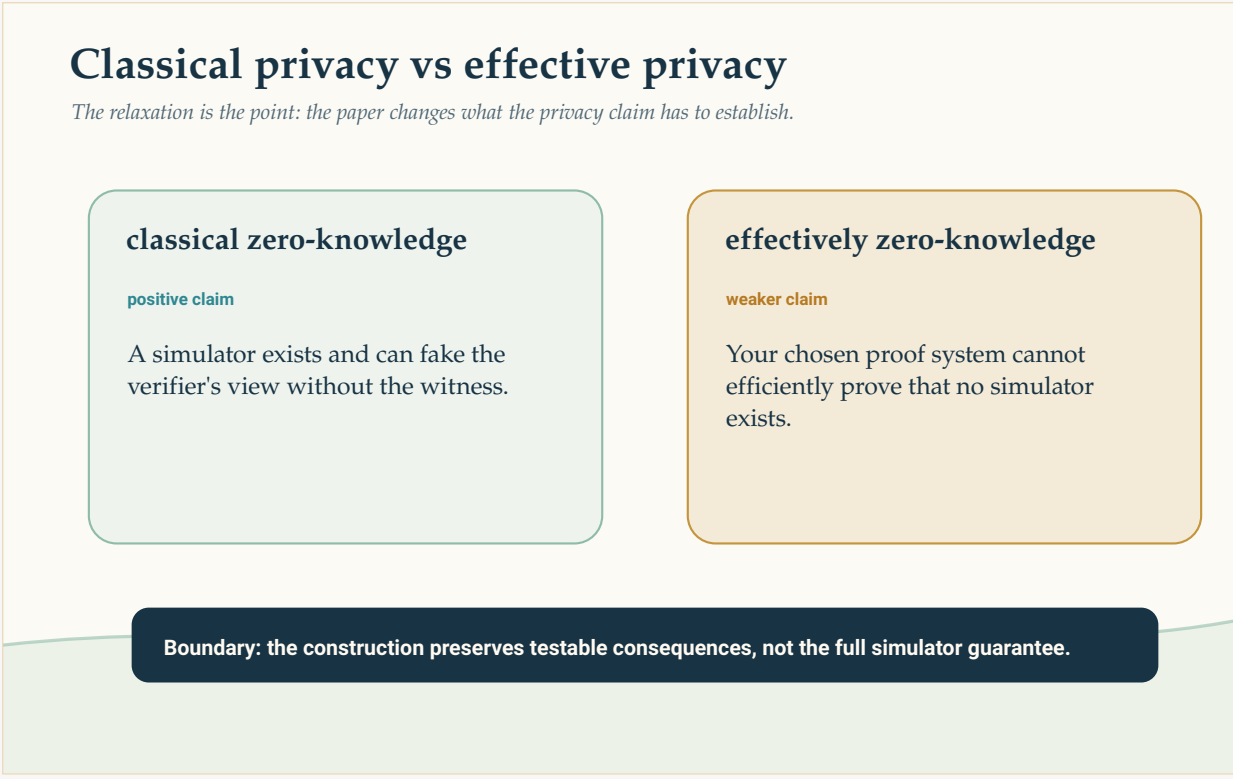
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



ნულოვანი ცოდნისკენ სამი გზა იკეტება — ინტერაქცია, სანდო სქემა და არასრულყოფილი სისწორე. ილანგოს კონსტრუქცია სხვა კარიდან გადის: არჩეულ ფორმალურ სისტემას არ შეუძლია ეფექტურად დაამტკიცოს, რომ სიმულატორი შეუძლებელია.

Classical privacy vs effective privacy

The relaxation is the point: the paper changes what the privacy claim has to establish.



კლასიკური ნულოვანი ცოდნა ეკითხება, არსებობს თუ არა სიმულატორი; „ეფექტურად

ნულოვანი ცოდნა“ მხოლოდ იმას ეკითხება, შეუძლია თუ არა არჩეულ ფორმალურ წესთა სისტემას ეფექტურად დაამტკიცოს, რომ სიმულატორი არ არსებობს. სწორედ ეს უფრო სუსტი კითხვა აძლევს კონსტრუქციას საშუალებას შეინარჩუნოს ერთი შეტყობინება, სქემის არარსებობა და სრულყოფილი სისწორე.

ძველი ტესტი: სიმულატორი არსებობს

ნულოვანი ცოდნის კლასიკური ფორმალიზაცია იყენებს წარმოსახვით დამხმარეს, რომელსაც **სიმულატორი** ეწოდება.

იდეა ასეთია: წარმოვიდგინოთ ჯეინი, რომელმაც ალისის საიდუმლო **არ იცის**. თუ ჯეინს სრულიად დამოუკიდებლად შეუძლია ისეთი მტკიცებულებების გენერირება, რომლებიც ზუსტად ჰგავს იმას, რასაც ბობი ალისისგან მიიღებდა, მაშინ ალისის მტკიცებულებას ბობისთვის ახალი არაფერი უსწავლებია. ჯეინს ისედაც შეეძლო იგივე გამოცდილების გათამაშება ალისის საიდუმლოს გარეშე.

ამიტომ კლასიკური ნულოვანი ცოდნა ნამდვილ სიმულატორს მოითხოვს. უნდა არსებობდეს ეფექტური ალგორითმი, რომელსაც საიდუმლოს — ჟარგონით *მოწმის* — ცოდნის გარეშე შეუძლია დამაჯერებლად ისეთი მტკიცებულებების გენერირება, რომლებიც ნამდვილებს ჰგავს. სუდოკუში მოწმე უბრალოდ სრულად და სწორად შევსებული ბადეა.

ეს განსაზღვრება ძლიერია, მაგრამ სწორედ აქ ეჯახება ძველ შეუძლებლობას. ინტუიცია ასეთია: ნამდვილად არაინტერაქტიული მტკიცებულება უბრალოდ სიმბოლოების სტრიქონია. როგორც კი ბობს ეს სტრიქონი აქვს, მას შეუძლია სხვასაც აჩვენოს: მან მიიღო უნარი, განცხადება სხვა ადამიანებსაც დაუმტკიცოს, რაც უკვე „არაფრის“ მიღებაზე მეტს ჰგავს. კლასიკური თეორემები ამ ინტუიციას ზემოთ აღწერილ შეუძლებლობებამდე ამკაცრებს.

სამი თვისება, რომლებზეც ეს ნაშრომი უარს არ ამბობს

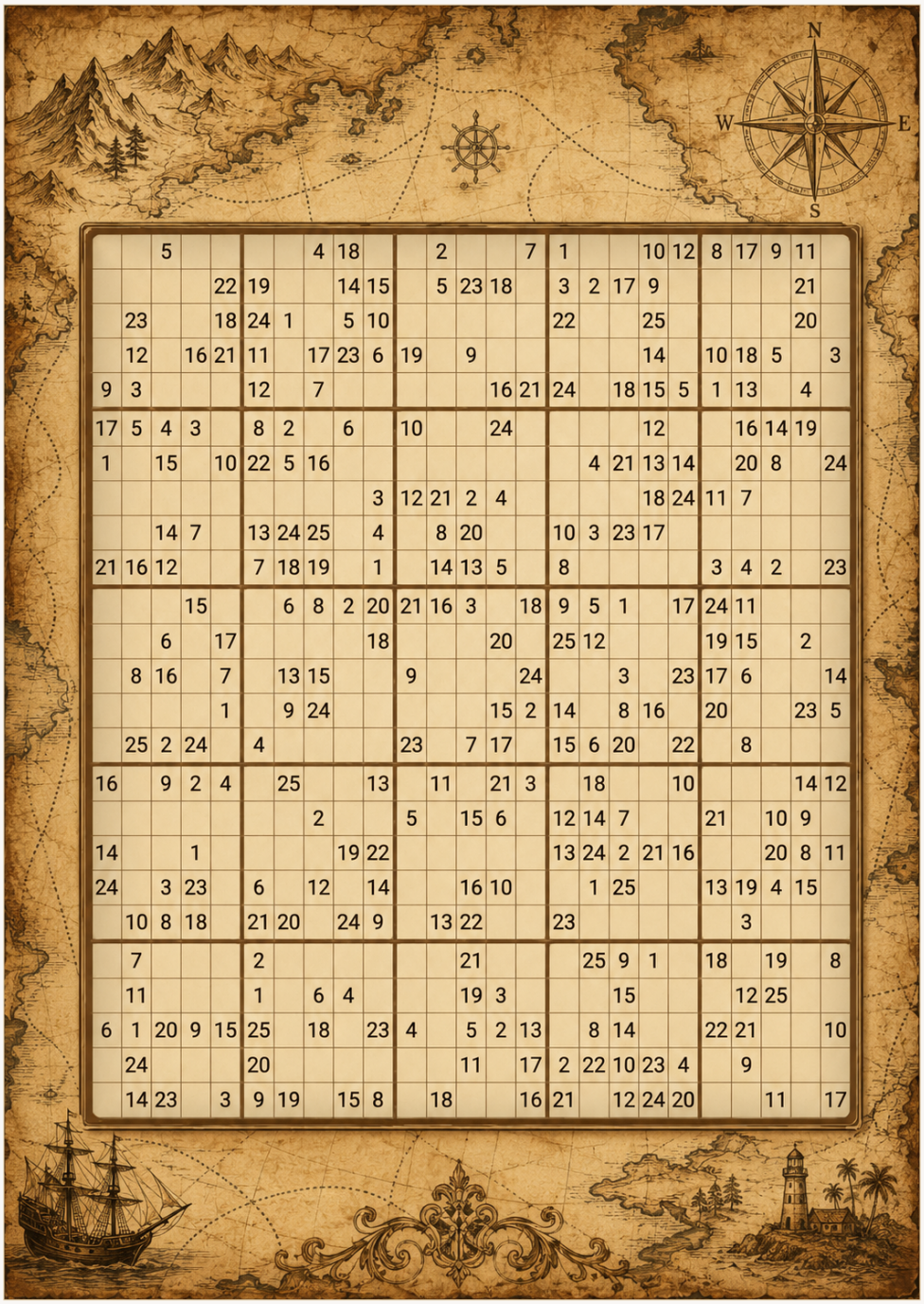
ნაშრომის სათაური სამ შეზღუდვას ასახელებს:
ინტერაქციის გარეშე: ალისი აგზავნის ერთ მტკიცებულების სტრიქონს. კითხვა-პასუხის პროტოკოლი არ არსებობს.
სქემის გარეშე: ალისი და ბობი არ ეყრდნობიან სანდოდ გავრცელებულ საერთო სტრიქონს ან წინასწარ შეთანხმებულ საჯარო შემთხვევითობას. ბევრ სისტემას, რომელსაც „არაინტერაქტიულ ნულოვან ცოდნას“ უწოდებენ, ასეთი მოსამზადებელი სქემა მაინც სჭირდება; აქ კი სქემა საერთოდ არ არის.
სრულყოფილი სისწორე: მცდარ განცხადებას ვალიდური მტკიცებულება არ აქვს. არა „თითქმის არასოდეს მიიღება“, არამედ — ვალიდური მტკიცებულება საერთოდ არ არსებობს.
ეს ზუსტად ის სამი თვისებაა, რომელიც ჩვეულებრივ წერილობით მათემატიკას

> აქვს — და, როგორც ზემოთ ვნახეთ, კლასიკური ნულოვანი ცოდნა მათ ერთად ვერ ინარჩუნებს.

განსხვავება მეგა-სუდოკუს ენაზე

აი, განზრახ გამარტივებული გზა, რომ განსხვავება ინტუიციურად დავინახოთ.

სერიოზული ანალოგიისთვის ჩვეულებრივი 9×9 სუდოკუ არ გამოგვადგება. ის ზედმეტად პატარა და სასრულია: კომპიუტერს შეუძლია უბრალოდ ამოხსნას ან დაამტკიცოს, რომ ამოხსნა არ აქვს. ამის ნაცვლად წარმოვიდგინოთ **MegaSudoku(n)** ამოცანების ოჯახი. გავზარდოთ ჩვეულებრივი წესი: ავირჩიოთ ბლოკის ზომა n, დავაყენოთ $N = n^2$ და ავაგოთ $N \times N$ ბადე, დაყოფილი $n \times n$ ბლოკებად და N სიმბოლოთი. ჩვეულებრივი სუდოკუ მხოლოდ პატარა შემთხვევაა, $n = 3$, $N = 9$: 9×9 ბადე, 3×3 ბლოკები და ცხრა სიმბოლო. მტკიცებულებათა სირთულის ისტორია იწყება მაშინ, როცა n იზრდება და ბადეს ემატება ისეთი კონსტრუქციები, რომლებიც მას სუდოკუს ფორმით ჩაწერილ SAT ამოცანად აქცევს. SAT ფორმულა კი უბრალოდ „კი/არა“ ტიპის შეზღუდვების ერთობლიობაა: შეიძლება თუ არა ცვლადებს ჭეშმარიტი ან მცდარი მნიშვნელობები მივანიჭოთ ისე, რომ ყველა შეზღუდვა შესრულდეს?



		5					4	18			2			7	1			10	12	8	17	9	11	
				22	19			14	15		5	23	18		3	2	17	9					21	
	23			18	24	1		5	10						22			25					20	
	12		16	21	11		17	23	6	19		9						14		10	18	5		3
9	3				12		7						16	21	24		18	15	5	1	13		4	
17	5	4	3		8	2		6		10			24					12			16	14	19	
1		15		10	22	5	16									4	21	13	14		20	8		24
									3	12	21	2	4					18	24	11	7			
		14	7		13	24	25		4		8	20			10	3	23	17						
21	16	12			7	18	19		1		14	13	5		8					3	4	2		23
			15			6	8	2	20	21	16	3		18	9	5	1		17	24	11			
		6		17					18				20		25	12				19	15		2	
	8	16		7		13	15			9				24			3		23	17	6			14
				1		9	24						15	2	14		8	16		20			23	5
	25	2	24		4					23		7	17		15	6	20		22		8			
16		9	2	4		25			13		11		21	3		18			10				14	12
							2			5		15	6		12	14	7			21		10	9	
14			1					19	22						13	24	2	21	16			20	8	11
24		3	23		6		12		14			16	10			1	25			13	19	4	15	
	10	8	18		21	20		24	9		13	22			23						3			
	7				2							21				25	9	1		18		19		8
	11				1		6	4				19	3				15				12	25		
6	1	20	9	15	25		18		23	4		5	2	13		8	14			22	21			10
	24				20							11		17	2	22	10	23	4		9			
	14	23		3	9	19		15	8		18			16	21		12	24	20			11		17

25×25 სუდოკუ: მისი წესების შემოწმება შესაძლებელია დასრულებული ბადის გაუმჟღავნებლად — ვიზუალური ანალოგი მტკიცებულებისა, რომელიც დაფარულ ამოხსნას, witness-ს, ამოწმებს.

სუდოკუ და SAT: ერთი თავსატეხი ორი სამოსით

მტკიცება, რომ სუდოკუ შეიძლება „SAT ფორმულასავით იქცეოდეს“, მეტაფორა არ არის. გარდაქმნა ორივე მიმართულებით მუშაობს, ხოლო მარტივი მიმართულება სრულადაც შეიძლება ჩამოვწეროთ.

სუდოკუდან SAT-მდე. SAT მხოლოდ ჭეშმარიტი/მცდარი მნიშვნელობებით ოპერირებს, ამიტომ მივცეთ თითო ბულური ცვლადი ყოველ (მწკრივი, სვეტი, მნიშვნელობა) სამეულს: *x(r,c,v)* ნიშნავს „*r* მწკრივის, *c* სვეტის უჯრაში წერია *v*“. 4×4 სუდოკუსთვის (2×2 ბლოკები, მნიშვნელობები 1–4) საჭიროა 4·4·4 = 64 ცვლადი; კლასიკური 9×9-ისთვის — 729. შემდეგ სუდოკუს ყველა წესი კლაუზების ჯგუფად გარდაიქმნება. (კლაუზა არის ცვლადების ან მათი უარყოფების OR; მთელი ფორმულა ყველა კლაუზის AND-ია.)
ყოველ უჯრაში მინიმუმ ერთი მნიშვნელობაა — თითო clause ყოველ უჯრაზე:

x(1,1,1) ∨ x(1,1,2) ∨ x(1,1,3) ∨ x(1,1,4)

ყოველ უჯრაში მაქსიმუმ ერთი მნიშვნელობაა — მნიშვნელობების ყოველი წყვილისთვის „ორივე ერთად არა“ clause:

¬x(1,1,1) ∨ ¬x(1,1,2) ¬x(1,1,1) ∨ ¬x(1,1,3) … და ასე ექვსივე წყვილისთვის.

ყოველი მწკრივი ყველა მნიშვნელობას შეიცავს — პირველი მწკრივისა და 3-ისთვის: მინიმუმ ერთხელ,

x(1,1,3) ∨ x(1,2,3) ∨ x(1,3,3) ∨ x(1,4,3)

და მაქსიმუმ ერთხელ: ¬x(1,1,3) ∨ ¬x(1,2,3), და ასე მწკრივის უჯრების ყოველი წყვილისთვის.
სვეტები და ბლოკები — იგივე ტიპის ჯგუფებია; იცვლება მხოლოდ უჯრების ჯგუფი. ზედა მარცხენა ბლოკისა და მნიშვნელობა 2-ისთვის:

x(1,1,2) ∨ x(1,2,2) ∨ x(2,1,2) ∨ x(2,2,2)

და ამას ემატება ყველა წყვილის „ორივე ერთად არა“ clause.
დაბეჭდილი მინიშნებები — ყველაზე მარტივი ნაწილი: ყოველი მინიშნება ერთცვლადიანი clause-ია. ზედა მარცხენა კუთხეში დაბეჭდილი 3 ხდება

x(1,1,3)

ყველა ამ კლაუზის AND დაკმაყოფილებადია ზუსტად მაშინ, როცა სუდოკუს ამოხსნა აქვს — და დამაკმაყოფილებელი მინიჭება თავადაც *ამოხსნაა*: ვნახოთ, რომელი x(r,c,v)-ებია ჭეშმარიტი და შევავსოთ ბადე. 9×9 შემთხვევაში ეს 729 ცვლადსა და რამდენიმე ათას კლაუზას იძლევა, რასაც თანამედროვე SAT ამომხსნელი მილიწამებში უმკლავდება. ყურადღება მიაქციეთ მინიშნების კლაუზას x(1,1,3): ის ამბობს „ეს უჯრა ზუსტად 3-ის ტოლია“ და არა „ეს უჯრები ერთმანეთისგან განსხვავდება“ — სწორედ ეს ასიმეტრია მოითხოვს დამატებით ხრიკს მინიშნების უჯრებისთვის ქვემოთ აღწერილ პროტოკოლში.
SAT-დან სუდოკუმდე. ნაშრომს საპირისპირო, უფრო რთული მიმართულება სჭირდება: ავიღოთ *ნებისმიერი* SAT ფორმულა და ავაგოთ მეგა-სუდოკუ, რომელსაც ამოხსნა აქვს ზუსტად მაშინ, როცა ფორმულაც დაკმაყოფილებადია.

სუდოკუს ბუნებრივი წესები მხოლოდ იმას ამბობს, რომ „ეს უჯრები ერთმანეთისგან განსხვავდება“, ამიტომ ნებისმიერი ლოგიკური შეზღუდვა *ასაგებია* — სწორედ ამას აკეთებს კონსტრუქცია. ეს არის უჯრების პატარა, წინასწარ შემუშავებული კლასტერი თითო ფორმულის კლაუზაზე, სადაც კონკრეტული უჯრები ცვლადების როლს ასრულებს (მათში ჩაწერილი სიმბოლო ჭეშმარიტს ან მცდარს კოდავს), ხოლო შიდა შეზღუდვები ისეა აგებული, რომ ლეგალური შევსებები ზუსტად ამ კლაუზის დამაკმაყოფილებელ მინიჭებებს შეესაბამებოდეს. ეს NP-სრულობის მტკიცებულებების სტანდარტული ტექნიკაა; განზოგადებული Sudoku-სთვის ის Yato-მ და Seta-მ 2003 წელს განახორციელეს. ორივე მიმართულება ერთად ამბობს, რომ N×N Sudoku და SAT ერთი პრობლემა სხვადასხვა სამოსშია. სწორედ ამიტომ შეუძლია ამ სტატიას — და ნაშრომსაც — მთელი NP-ის ისტორია ბადეებითა და სიმბოლოებით მოყვეს.

მოწმის წარმოდგენა მაინც მარტივია. ალისმა იცის მეგა-სუდოკუს სრული, სწორი შევსება. ბობს სურს დარწმუნდეს, რომ ასეთი შევსება არსებობს, მაგრამ ალისს მისი გამჟღავნება არ უნდა. თუ სრულ ბადეს გაუგზავნის, ბობი დარწმუნდება, თუმცა საიდუმლო გაქრება.

კლასიკურ ნულოვანი ცოდნა ვერსიაში ალისი და ბობი ურთიერთქმედებენ. ერთ ძველ ინტუიციურ მოდელში დაფარული ფილები გამოიყენება. ალისი მალავს ამოხსნილ ბადეს, ყოველი რაუნდის წინ სიმბოლოებს საიდუმლოდ გადაარქმევს და ბობს საშუალებას აძლევს შემთხვევით შერჩეული ერთი ლოკალური შეზღუდვა შეამოწმოს: მწკრივი, სვეტი, ბლოკი ან კონსტრუქცია. თუ გახსნილ უჯრებში ყველა სიმბოლო განსხვავებულია, ბობის ნდობა იზრდება. შემდეგ ყველაფერი ისევ იფარება და სიმბოლოებს ახალი სახელები ეძლევა. (ერთი სირთულე არსებობს: დაბეჭდილ მინიშნებებს დამატებითი ხრიკი სჭირდება, რადგან სიმბოლოების გადარქმევა მათაც ფარავს. ქვემოთ მოცემული შენიშვნა ხსნის, როგორ უმკლავდება ამას კლასიკური პროტოკოლი; ჩვენი გამარტივებული სურათისთვის ეს საკმარისია.)

როგორ ამოწმებენ კლასიკური პროტოკოლები მინიშნება-უჯრებს სინამდვილეში

სიმბოლოების გადარქმევის ხრიკს ბრმა წერტილი აქვს. მწკრივის, სვეტის და ბლოკის ყველა წესი ამბობს „ეს უჯრები ერთმანეთისგან განსხვავდება“, ხოლო *ყველა განსხვავებულია* ნებისმიერ გადარქმევას უძლებს. მაგრამ მინიშნება ამბობს „ამ უჯრაში ზუსტად 5 წერია“, გადარქმევის შემდეგ კი ბობი მხოლოდ $\sigma(5)$-ს — რაღაც შენიღბულ სიმბოლოს — ხედავს და σ გარდაქმნა არ იცის. ამიტომ ვერაფერს ამოწმებს. თუ ეს პრობლემა არ მოგვარდება, ალისს შეუძლია დაამტკიცოს, რომ *რაღაც* სწორი ბადე არსებობს, დაბეჭდილი მინიშნებების სრული იგნორირებით — რაც *ამ კონკრეტულ* თავსატეხზე არაფერს ამტკიცებს. კლასიკურ ლიტერატურაში ორი სტანდარტული გამოსავალია.

პალიტრა. დამალულ ბადეს დაემატოს N უჯრის ერთი დამატებითი მწკრივი — პალიტრა, რომელსაც ალისი საჯაროდ განსაზღვრული თანმიმდევრობით ავსებს

სიმბოლოებით 1…N და შემდეგ, დანარჩენთან ერთად, გადაარქმევს, ამიტომ მასში გვაქვს $\sigma(1)\ldots\sigma(N)$. ახლა ბობის შემთხვევით გამოწვევას დამატებითი ვარიანტი აქვს. მწკრივის, სვეტის, ბლოკის ან კონსტრუქციაის გახსნის გარდა, შეუძლია მოითხოვოს **პალიტრა და ერთი მინიშნება-უჯრა**. ალისი ორივეს ხსნის; პალიტრა ამ რაუნდის გადარქმევას აჩენს, ხოლო ბობი ამოწმებს, რომ მინიშნება-უჯრაში დაბეჭდილი მნიშვნელობის ზუსტად გადარქმეული ვერსია წერია. ნულოვანი ცოდნა შენარჩუნებულია, რადგან ბობი მხოლოდ σ-ს იგებს — რომელიც ყოველ რაუნდში თავიდან შემთხვევითად აირჩევა და თავისთავად არაფერს ამხელს — და იმ უჯრის მნიშვნელობას, რომელიც თავსატეხიდან ისედაც იცოდა. საიდუმლო უჯრებზე არაფერი ჟონავს, ხოლო სიმულატორს იგივე სურათის გაყალბება შემთხვევითი σ-ს არჩევით შეუძლია. სისწორე მიიღება იმიტომ, რომ მოტყუებული ალისი ყოველ რაუნდში ფიქსირებული ალბათობით შეიძლება გამოიჭიროს, ხოლო რაუნდები მეორდება მანამ, სანამ ეჭვის ალბათობა უმნიშვნელო გახდება.

მინიშნებების „კომპილირება“. უფრო სტრუქტურული ვარიანტი სპეციალურ გამოწვევას კი არ ამატებს, არამედ საერთოდ შლის მის საჭიროებას. მინიშნება-ის მნიშვნელობის *შემოწმების* ნაცვლად იგი განსხვავების შეზღუდვებით იძულებით განისაზღვრება: მინიშნება-უჯრა დაუკავშირეთ პალიტრის ყველა უჯრას, გარდა იმ უჯრისა, რომელიც მის საკუთარ მნიშვნელობას ატარებს — „განსხვავდება $\sigma(1)$-ისგან, განსხვავდება $\sigma(2)$-ისგან, …, განსხვავდება ყველაფრისგან $\sigma(5)$-ის გარდა“. ამ უჯრაში ლეგალურად მხოლოდ მინიშნება-ის სიმბოლო შეიძლება დარჩეს. ყველა შეზღუდვა ისევ „ეს ორი განსხვავდება“ ტიპისაა — გადარქმევის მიმართ უცვლელი და მწკრივის წესივით შემოწმებადი. იგივე ხრიკი გამოიყენება pre-colored vertex-ებისთვის კლასიკურ graph-coloring protocol-ში და სწორედ ასეთია ზემოთ ნახსენები *კონსტრუქცია*-ების იდეაც: MegaSudoku-as-SAT სურათში მინიშნება-ები ყველა სხვა შეზღუდვის მსგავს inequality კონსტრუქცია-ებად კომპილირდება.

ფიზიკური პროტოკოლი. Sudoku-ს რეალური ბარათების პროტოკოლი (Gradwohl, Naor, Pinkas და Rothblum, 2007) საერთოდ არ იყენებს გადარქმევას და მინიშნებებს დამალვამდე ასწორებს. თითოეული უჯრისთვის ალისი დებს ერთნაირი მნიშვნელობის სამ ბარათს — საიდუმლო უჯრებისთვის პირქვე, მაგრამ **მინიშნების უჯრებისთვის პირაღმა**, რათა ბობმა საკუთარი თვალით ნახოს, რომ მინიშნებები დაცულია, სანამ ბარათები გადაიფარება. შემდეგ თითო უჯრიდან ერთი ბარათი მიდის მისი მწკრივის პაკეტში, ერთი — სვეტისაში და ერთი — ბლოკისაში; თითოეული პაკეტი ირევა და იხსნება, ბობი კი ამოწმებს, რომ მასში ყველა N სიმბოლოა. არევა პოზიციურ ინფორმაციას ანადგურებს — სწორედ ეს უზრუნველყოფს ნულოვან ცოდნას — ხოლო მინიშნებები უკვე წინასწარ იყო დაფიქსირებული.

ნებისმიერ შემთხვევაში გაკვეთილი იგივეა, რომელსაც ეს სტატია კვლავ და კვლავ უბრუნდება: ნულოვანი ცოდნის პროტოკოლი ყურადღებით აღრიცხავს, *რომელი* ფაქტები გადაურჩება დამალვას. გადარქმევა ინარჩუნებს „ყველა განსხვავებულია“-ს და შლის „ზუსტად 5-ის ტოლია“-ს — ამიტომ „ზუსტად 5-ის ტოლია“ სხვა გზით უნდა დაბრუნდეს.

ეს ნაშრომში გამოყენებული პროტოკოლი არ არის. ეს კლასიკური ნულოვანი ცოდნის ინტუიციური მოდელია:

- ალისი და ბობი ერთმანეთთან მრავალჯერ ურთიერთობენ.
- ბობი შემთხვევით შემოწმებებს ირჩევს.
- ალისი მხოლოდ ლოკალურ თანმიმდევრულობას ამჟღავნებს და არა სრულ ამოხსნას.
- კონფიდენციალურობის მტკიცებულება ეფუძნება იმას, რომ ბობის მიღებული სურათი ალისის საიდუმლო ამოხსნის გარეშე შეიძლებოდა გენერირებულიყო.

ამიტომ კლასიკური ნულოვანი ცოდნა ერთ დადებით ფაქტზე დგას:

> სიმულატორი ნამდვილად არსებობს.

ახლა ეს კომფორტული ნაწილები მოვაშოროთ. ალისი ერთ მტკიცებულების სტრიქონს აგზავნის და მიდის. სანდო სქემა არ არსებობს, წინასწარ მომზადებული საერთო შემთხვევითი სტრიქონიც არაა, და ბობმა მცდარი თავსატეხი არასოდეს უნდა მიიღოს. სწორედ ამ გარემოში კლასიკური ნულოვანი ცოდნა ვერ ძლებს.

ხრიკის გასაგებად კიდევ ერთი პერსონაჟი გვჭირდება. წინასწარ დავაფიქსიროთ **წესთა წიგნი** — ლოგიკოსების ენაზე ფორმალური მტკიცებულებათა სისტემა: აქსიომების ფიქსირებული ნაკრები და წერილობითი მათემატიკური მტკიცებულებების მექანიკურად შესამოწმებელი წესები. კანონიერი მაგალითია ZFC, თანამედროვე მათემატიკის სტანდარტული აქსიომები. აქედან მოყოლებული ყველაფერი წინასწარ არჩეულ ასეთ სისტემასთან მიმართებით ფორმულირდება, არჩევანი კი მოქნილია: კონსტრუქცია მუშაობს ნებისმიერ წინასწარ დაფიქსირებულ სისტემაზე, მათ შორის ZFC-ზე.

(ტერმინოლოგიური შენიშვნა, როგორც თავად ნაშრომშია: აქ „მტკიცებულებათა სისტემა“ ყოველთვის ნიშნავს ამ ფორმალურ წესთა წიგნს — სისტემას, რომელიც მათემატიკურ მტკიცებულებებს ამოწმებს — და არასოდეს ალისის მიერ გაგზავნილ შეტყობინებებს. ალისისა და ბობის მექანიზმებს ეწოდება „დამმტკიცებელი“ და „შემმოწმებელი“.)

გიოდელის სტილის ვერსია მეგა-სუდოკუს ამბავს ინარჩუნებს, მაგრამ მტკიცებულებას ცვლის.

ავიღოთ იგივე ნაჩვენები ზომის მეორე შეზღუდვათა სისტემა და დავარქვათ **D**. ჩვენი ამბისთვის S და D ერთ ფორმატში ჩაწერილი ორი MegaSudoku(n) ამოცანაა. კულისებს მიღმა D შესაძლოა სხვა ზომის რთული ლოგიკური ფორმულიდან დაიწყო; საჭიროების შემთხვევაში მას უვნებელი დამატებითი შეზღუდვები ემატება, რათა იმავე ბადეში ჩაეტიოს. D აგებულია ლოგიკური ფორმულისგან, რომელიც სინამდვილეში **დაუკმაყოფილებადია**: არ არსებობს მნიშვნელობების ისეთი მინიჭება, რომელიც მის ყველა შეზღუდვას დააკმაყოფილებს — ისევე, როგორც გაფუჭებულ თავსატეხს ლეგალური სრული ბადე არ აქვს. სათამაშო მაგალითი იქნებოდა ფორმულა, რომელიც ერთდროულად მოითხოვს „X არის ჭეშმარიტი“ და „X არის მცდარი“. ამიტომ D-ს სწორი შევსება არ აქვს.

მაგრამ D ისეთი გატეხილი თავსატეხი არ უნდა იყოს, რომლის სიყალბეც *ადვილად დასამტკიცებელია*. ზემოთ მოყვანილი სათამაშო მაგალითი სწორედ ამიტომ არ გამოდგება: ნებისმიერი ფორმალური სისტემა „X და არა-X“-ს ერთ ხაზში უარყოფს. D მცდარი უნდა იყოს ისეთი გზით, რომლის მოკლე დასაბუთებასაც არჩეული სისტემა ვერ იძლევა. თუ წესთა წიგნს D-ის მოკლე უარყოფა შეეძლებოდა, ქვემოთ აღწერილი იდეა დაიშლებოდა: ალისის რეალური საიდუმლოს გარეშე მტკიცებულების შექმნის ალტერნატიული გზა ფორმალურად გამოირიცხებოდა და მასთან ერთად — კონფიდენციალურობის გარანტიაც. ამიტომ D ირჩევა ისეთი ოჯახიდან, რომლის ეფექტურად უარყოფა ფიქსირებულ სისტემას არ შეუძლია: ამ სისტემის შიგნით არ არსებობს მოკლე მტკიცებულება, რომ D-ს ამოხსნა არ აქვს.

ალისის ერთშეტყობინებიანი მტკიცებულება შემდეგი „ან/ან“ განცხადების შესახებ არის:

> ან რეალურ მეგა-სუდოკუ S-ს აქვს ამოხსნა, ან სატყუარა D-ს აქვს ამოხსნა.

სწორედ ესაა ლოგიკური კავშირი. D რაღაც ჯადოსნური გზით არ გენერირდება S-ის გასაჭეშმარიტებლად. მტკიცებულება არ ამბობს „D-ს ამოხსნა არ აქვს, მაშასადამე S-ს აქვს“. ის ამტკიცებს დისიუნქციას **S ან D**. სრულყოფილი სისწორე ნიშნავს, რომ მცდარ დისიუნქციას ვალიდური მტკიცებულება არ აქვს. რადგან რეალურად D მცდარია — ამოხსნა არ აქვს — დისიუნქცია ჭეშმარიტი მხოლოდ მაშინ შეიძლება იყოს, თუ S ჭეშმარიტია. ამიტომ მიღებული მტკიცებულება ნიშნავს, რომ S-ს ამოხსნა აუცილებლად აქვს. სატყუარა მცდარ S-ს ჭეშმარიტად ვერ აქცევს.

მაგრამ ნულოვანი ცოდნის მსგავსი ნაწილისთვის ვიკითხოთ, რა მოხდებოდა, D-ს *რომ ჰქონოდა* ამოხსნა. ეს სატყუარა ამოხსნა ალტერნატიული მოწმე იქნებოდა. მისი გამოყენებით შესაძლებელი გახდებოდა მტკიცებულებების შექმნა ალისის ნამდვილი მეგა-სუდოკუს ამოხსნის ცოდნის გარეშე — სხვა სიტყვებით, სიმულატორი იარსებებდა. რეალურად D-ს ამოხსნა არ აქვს, ამიტომ ეს გზა დახურულია. არსებითი ისაა, რომ არჩეულ სისტემას არ შეუძლია ეფექტურად დაამტკიცოს, რომ ეს გზა დახურულია.

ამრიგად, D-ს ორი საქმე აქვს. **სისწორისთვის** D მცდარია, ამიტომ „S ან D“-ის ვალიდური მტკიცებულება S-ს ჭეშმარიტებას აიძულებს. **ეფექტური ნულოვანი ცოდნისთვის** D-ის უარყოფა რთულია, ამიტომ წესთა წიგნი სწრაფად ვერ გამორიცხავს იმ სატყუარა გზას, რომელიც სიმულაციას შესაძლებელს გახდიდა.

ამიტომ უსაფრთხოების ტესტი აღარ არის:

> შეგვიძლია დავამტკიცოთ, რომ სიმულატორი ნამდვილად არსებობს?

ის ხდება:

> შეუძლია თქვენს წესთა წიგნს ეფექტურად დაამტკიცოს, რომ სიმულატორი შეუძლებელია?

თუ პასუხი უარყოფითია, მოულოდნელად ძლიერი შედეგი მიიღება: უსაფრთხოების ყოველი გარანტია, რომელიც (a) ტესტის გაშვებით დაკვირვებადია და (b) ამ წესთა წიგნის შიგნით დასამტკიცებლად გამომდინარეობს სიმულატორის არსებობიდან, რეალურად სრულდება. რომელიმე ასეთ თვისებაზე წარმატებული შეტევა თავად იქნებოდა ის დაკარგული მოკლე უარყოფა — ხოლო ეს მოკლე უარყოფა არ არსებობს. სწორედ ესაა სიტყვა „ეფექტურის“ აზრი ეფექტურ ნულოვან ცოდნაში.

საკლასო კონტრასტი ასეთია:

კლასიკური ნულოვანი ცოდნა: მტკიცებულებები უსაფრთხოა იმიტომ, რომ სიმულატორი არსებობს.

გიოდელის სტილის ეფექტური ნულოვანი ცოდნა: დაკვირვებადი უსაფრთხოების ტესტებისთვის მტკიცებულებებს უსაფრთხოდ ვთვლით, რადგან არჩეულ წესთა წიგნს არ შეუძლია ეფექტურად დაამტკიცოს, რომ სიმულატორი შეუძლებელია.

მეორე მტკიცება უფრო სუსტია. სწორედ ამიტომ შეუძლია ნაშრომს შეინარჩუნოს ის სამი თვისება, რომლებიც კლასიკურ ვერსიას არღვევდა: ერთი შეტყობინება, სქემის არარსებობა და სრულყოფილი სისწორე.

ახალი ტესტი: ვერ ამტკიცებ, რომ სიმულატორი არ არსებობს

ილანგოს მოდუნებული განსაზღვრება კითხვას ცვლის.

კლასიკური ნულოვანი ცოდნა ეკითხება:

> არსებობს სიმულატორი?

ეფექტურად ნულოვანი ცოდნა ეკითხება უფრო სუსტ რამეს:

> შეუძლია თქვენს არჩეულ წესთა წიგნს ეფექტურად დაამტკიცოს, რომ სიმულატორი არ არსებობს?

ეს შეიძლება ტექნიკურ თავის დაძვრენად ჟღერდეს, მაგრამ სწორედ ესაა ძირითადი იდეა. კონსტრუქცია უცნაურ მდგომარეობაში ცხოვრობს: სიმულატორი სინამდვილეში არ არსებობს — ნაშრომი ამას პირდაპირ ამბობს — მაგრამ თქვენ მიერ დაფიქსირებულ ფორმალურ სისტემას არ შეუძლია ეფექტურად დაამტკიცოს, რომ ის არ არსებობს. თუ ყველა არასასურველი შედეგი, რომლის თავიდან აცილებაც გვინდა, ასეთ უარყოფას მოითხოვს, სისტემა ამ შედეგებთან მიმართებით მაინც ნულოვანი ცოდნასავით იქცევა.

აქ შემოდის გიოდელი. არა დეკორაციისთვის და არა იმ აზრით, რომ „გიოდელი კრიპტოგრაფიას უსაფრთხოს ხდის“. კავშირი მტკიცებულებათა თეორიასთანაა.

წესთა წიგნს **ოპტიმალური** ეწოდება, თუ ის ზუსტი მნიშვნელობით საუკეთესო შესაძლო სისტემაა: როდესაც სხვა რომელიმე სისტემა შესაბამისი ტიპის ფორმულას მოკლე მტკიცებულებით უარყოფს, ოპტიმალურ სისტემასაც შეუძლია იგივე მაქსიმუმ პოლინომიურად გრძელი მტკიცებულებით. Krajíček-მა და Pudlák-მა 1989 წელს წამოაყენეს ვარაუდი, რომ **ოპტიმალური მტკიცებულებათა სისტემა არ არსებობს**: რომელ სისტემასაც არ უნდა ავირჩევდეთ, სხვა რომელიმე სისტემა ჭეშმარიტ განცხადებათა გარკვეულ ოჯახს ბევრად უფრო მოკლედ ამტკიცებს. ეს მტკიცებულებათა სირთულის ერთ-ერთი ცენტრალური ღია ვარაუდია და გიოდელის არასრულობის თეორემის სასრული, სირთულეზე ორიენტირებული ნათესავი: არსებობს ჭეშმარიტი განცხადებები, რომლებსაც თქვენ მიერ არჩეულ სისტემაში მოკლე მტკიცებულება არ აქვს — არა იმიტომ, რომ პრინციპში დაუმტკიცებელია, არამედ იმიტომ, რომ ყოველი ფიქსირებული სისტემა ზოგ მოკლე ჭეშმარიტებას მოკლე მტკიცებულების გარეშე ტოვებს.

ნაშრომი ამ ვარაუდს ეყრდნობა (ოდნავ უფრო ძლიერ „infinitely often“ ფორმაში, როგორც კრიპტოგრაფიაში გამოყენებისას ჩვეულებრივ ხდება). Krajíček–Pudlák-ის თეორემის წყალობით შედეგი კონკრეტულია: ყოველი წესთა წიგნისთვის არსებობს ფორმულების მიმდევრობა, რომლებიც რეალურად დაუკმაყოფილებადია, მაგრამ ამ სისტემას მათი მოკლე უარყოფა არ აქვს — და, გადამწყვეტად, მათი *გენერირება ეფექტურ ალგორითმს შეუძლია*. ეს ერთგვაროვნება იდეას არსებობის აბსტრაქტული მტკიცებიდან რეალურ ალგორითმად აქცევს, რომელსაც ალისი გაუშვებს: მისი სატყუარა D-ები კონსტრუქციულად გენერირდება და ჰაერიდან არ ჩნდება.

კრიპტოგრაფიული ნაბიჯი სწორედ ამ შეზღუდული მტკიცების უნარის გამოყენებაა.

რას აკეთებს კონსტრუქცია

ნაშრომის კონსტრუქცია, მხოლოდ ჩონჩხამდე დაყვანილი, ასეთია.

დააფიქსირეთ წესთა წიგნი — მაგალითად ZFC. მტკიცებულებათა სირთულის დაშვების პირობებში არსებობს ეფექტურად გენერირებადი ფორმულების მიმდევრობა, რომლებიც რეალურად დაუკმაყოფილებადია, მაგრამ წესთა წიგნს მათი დაუკმაყოფილებადობის მოკლე მტკიცებულება არ აქვს.

ახლა ავაგოთ ერთშეტყობინებიანი მტკიცებულება ასეთი ფორმით:

> ან რეალური განცხადება დაკმაყოფილებადია, ან ეს სპეციალური რთული ფორმულაა დაკმაყოფილებადი.

სპეციალური რთული ფორმულა სინამდვილეში დაკმაყოფილებადი არ არის. ამიტომ, თუ ძირითადი მტკიცების მექანიზმი სრულყოფილად სწორია, შეტყობინების მიღება მაინც ნიშნავს, რომ რეალური განცხადება ჭეშმარიტია. ასე მიიღება სრული სისწორის გარანტია.

მაგრამ ნულოვანი ცოდნის მსგავსი უსაფრთხოებისთვის წარმოვიდგინოთ, რომ

სპეციალური რთული ფორმულა *დაკმაყოფილებადი ყოფილიყო*. მაშინ მისი მოწმე შესაძლებელს გახდიდა მტკიცებულებების სიმულირებას რეალური მოწმის ცოდნის გარეშე. ფორმულა რეალურად დაკმაყოფილებადი არ არის — მაგრამ წესთა წიგნს ამის ეფექტურად დამტკიცება არ შეუძლია. შესაბამისად, მას ეფექტურად ვერც იმის დამტკიცება შეუძლია, რომ სიმულატორი შეუძლებელია.

სწორედ ესაა საკვანძო წერტილი. სისტემა საიდუმლოს კლასიკური სიმულატორის შექმნით არ მალავს. დაკვირვებადი უსაფრთხოების ტესტების ფართო კლასისთვის ის საიდუმლოს ფარავს წესთა წიგნის უუნარობის უკან — უუნარობის, რომ სიმულატორის არარსებობა დაადასტუროს.

რას ამტკიცებს ნაშრომი

მთავარი თეორემა რამდენიმე ფენად მოდის. ძირითადი შედეგი ასეთია:

სტანდარტული კრიპტოგრაფიული დაშვების — **არაინტერაქტიული მოწმის განურჩეველი მტკიცებულებების** არსებობის, კარგად შესწავლილი ობიექტებისა, რომლებიც რამდენიმე დამკვიდრებული დაშვების პაკეტიდან მიიღება — და მტკიცებულებათა სირთულის ვარაუდის, რომ **(infinitely often) ოპტიმალური მტკიცებულებათა სისტემა არ არსებობს**, პირობებში ნაშრომი ყოველი არჩეული წესთა წიგნისთვის აგებს NP/SAT-ის ერთშეტყობინებიან დამმტკიცებელსა და შემმოწმებელს **სრული სისწორის გარანტიით**, სქემის გარეშე, რომელიც ამ სისტემასთან მიმართებით ეფექტურად ნულოვანი ცოდნაა. (NP/SAT თავსატეხის ტიპის პრობლემების სტანდარტული „ყველაზე რთული საერთო მნიშვნელი“ა; მეგა-სუდოკუ მისი ერთ-ერთი სამოსია.)

უფრო ფართო მტკიცებისთვის — ფალსიფიცირებადი უსაფრთხოების თვისებების შენარჩუნებაზე — ნაშრომი კიდევ ერთ სტანდარტულ დაშვებას ამატებს, derandomization-ის რწმენას **P = BPP** (უხეშად: შემთხვევითობა ალგორითმებს არსებით დამატებით ძალას არ აძლევს).

თეორემის ენიდან ჩვეულებრივ ენაზე გადმოტანით:

- მტკიცებულება ერთი შეტყობინებაა.
- სანდო სქემა არ არსებობს.
- მცდარი განცხადებების დამტკიცება შეუძლებელია.
- დამმტკიცებელი კლასიკური ნულოვანი ცოდნა არ არის — მას სიმულატორი არ ჰყავს.
- მაგრამ კლასიკური ნულოვანი ცოდნის ყოველი ფალსიფიცირებადი, თამაშზე დაფუძნებული უსაფრთხოების შედეგის მიღება ამ გარემოში შესაძლებელია.

„ფალსიფიცირებადი“ მნიშვნელოვანია. ეს ნიშნავს, რომ უსაფრთხოების ჩავარდნა მოწინააღმდეგის თამაშში გაშვებით შეიძლება შემოწმდეს. მრავალი კრიპტოგრაფიული უსაფრთხოების განსაზღვრება სწორედ ასეთია: შეუძლია თუ არა მოწინააღმდეგეს ორი შიფროტექსტის გარჩევა, ფუნქციის ინვერსია, მოწმის აღდგენა ან კონკრეტული

ექსპერიმენტის მოგება? თეორემა თითო ფალსიფიცირებადი თვისებისთვის ცალკე დამმტკიცებელს იძლევა. ერთი დამმტკიცებელი, რომელიც *ყველა* ფალსიფიცირებად თვისებას ერთდროულად ფლობს, სავარაუდოდ შეუძლებელია — ძველი ხელახლა გამოყენების შეტევა („ბობს შეუძლია მტკიცებულება სხვას აჩვენოს“) თავადაც ფალსიფიცირებადი თვისებაა და აქ მართლაც ვერ სრულდება. ნაშრომი ვარაუდობს, რომ ერთმა დამმტკიცებელმა შეიძლება მოიცვას ყველა *ბუნებრივი* ფალსიფიცირებადი თვისება — ის თვისებები, რომლებიც კრიპტოგრაფიულ პრაქტიკაში რეალურად გვხვდება — მაგრამ ეს ნაწილი პირობითი თეორემაა, რომელიც „ბუნებრივის“ არაფორმალურ ცნებასა და დამატებით აშკარა ვარაუდს ეყრდნობა. გარანტია დაკვირვებად ჩავარდნებს ეხება და არა საიდუმლოების ყველა ფილოსოფიურ ან სიმულაციაზე დაფუძნებულ მნიშვნელობას.

ერთი კონკრეტული შედეგი აღნიშვნის ღირსია: კონსტრუქცია გვაძლევს პირველ არაინტერაქტიულ *მოწმის დამალვის* მტკიცებულებებს ერთგვაროვანი დამმტკიცებლით — „თავსატეხის მტკიცებულება მის ამოხსნაში არ გეხმარება“ — ინტერაქციისა და სქემის გარეშე. ეს თითქოს მოკრძალებული ობიექტია, რომლის აგებაც ათწლეულების განმავლობაში ვერ ხერხდებოდა.

რას არ ამბობს ეს ნაშრომი

ეს არის ნაწილი, რომელიც ტექსტს ზღვარს უყენებს.

ის **არ** ამბობს, რომ ძველი შეუძლებლობის თეორემები მცდარი იყო. კონსტრუქცია მათ განსაზღვრების შეცვლით უვლის გვერდს.

ის **არ** გვაძლევს ჩვეულებრივ, კლასიკურ ნულოვან ცოდნას ინტერაქციის გარეშე, სქემის გარეშე და სრული სისწორის გარანტიით. ნაშრომი პირდაპირ ამბობს, რომ აგებულ დამმტკიცებელს სიმულატორი არ აქვს.

ის **არ** ნიშნავს, რომ მტკიცებულების ხელახლა გამოყენება შეუძლებელია. ერთშეტყობინებიანი მტკიცებულება შეიძლება სხვასაც აჩვენო; ნაშრომი deniability-ის ტიპის თვისებებს არ ინარჩუნებს. (სანდო სქემაზე დაფუძნებულ არაინტერაქტიული ნულოვანი ცოდნასაც იგივე შეზღუდვა აქვს.)

ის **არ** ნიშნავს, რომ ეს დანერგვისთვის მზად პრაქტიკული პროტოკოლია. ეს სირთულის თეორიასა და კრიპტოგრაფიის საფუძვლებს ეხება. შედეგი მტკიცებულებათა სირთულისა და კრიპტოგრაფიის მნიშვნელოვან დაშვებებს ეყრდნობა და აჩვენებს, პრინციპში რა არის შესაძლებელი.

ის **არ** აქცევს „გიოდელს“ ჯადოსნურ უსაფრთხოების ინსტრუმენტად. გიოდელთან კავშირი მოდის მტკიცებულებათა სისტემებიდან, ოპტიმალური მტკიცებულებათა სისტემებიდან და არასრულობის სასრული ანალოგებიდან. გამოსადეგი ინტუიცია არ არის „არასრულობა ჩემს პაროლს იცავს“. უფრო ზუსტად: თუ წესთა წიგნს არ შეუძლია ეფექტურად დაამტკიცოს, რომ სიმულატორი შეუძლებელია, უსაფრთხოების განსაზღვრებების დონეზე შეიძლება დაიბლოკოს შეტევები, რომელთა წარმატებაც

სწორედ ასეთ მტკიცებულებას მოითხოვდა.

რატომ არის მაინც საინტერესო

კრიპტოგრაფია ხშირად სირთულეს უსაფრთხოებად გარდაქმნის. ფაქტორიზაცია რთულია, ამიტომ RSA-ს ტიპის დაშვებები სასარგებლო ხდება. გისოსებზე დაფუძნებული ამოცანები რთულია, ამიტომ გისოსური კრიპტოგრაფია სასარგებლოა. აქ სირთულე უფრო უცნაურია: არა „საიდუმლოს გამოთვლა რთულია“, არამედ „რთულია დაამტკიცო, რომ გარკვეული მტკიცებულების ობიექტი ვერ იარსებებს“.

ამიტომ გამოიყურება ნაშრომი უჩვეულოდ. ის აქსიომებსა და წესთა წიგნებს თითქმის კრიპტოგრაფიულ რესურსებად განიხილავს. ჩვეულებრივი შეუძლებლობა სისწორესა და სიმულაციას შორის დაძაბულობას გვიჩვენებს. ილანგოს ნაბიჯი ამ დაძაბულობას მტკიცებულებათა თეორიის ფარდის უკან ათავსებს: სიმულატორი არ არსებობს, მაგრამ ფორმალურ სისტემას არ შეუძლია მისი არარსებობის ეფექტურად გამომჟღავნება.

მკითხველისთვის მოულოდნელი ის კი არ არის, რომ ეს დღევანდელ ნულოვანი ცოდნა სისტემებს შეცვლის. ალბათ პირდაპირ არ შეცვლის. მოულოდნელია, რომ მათემატიკური ლოგიკის შეზღუდვა კონსტრუქციულად შეიძლება გამოვიყენოთ: არა მხოლოდ როგორც კედელი, არამედ როგორც საფარი.

რამდენად ძლიერია მტკიცებულება?

ეს თეორემული ნაშრომია, ამიტომ „მტკიცებულება“ აქ სხვა რამეს ნიშნავს, ვიდრე ბიოლოგიის ან ასტრონომიის სტატიაში. კითხვა არაა, გამეორდა თუ არა ექსპერიმენტი. კითხვა ისაა, უჭერს თუ არა განსაზღვრებები, დაშვებები და მტკიცების ჯაჭვი მხარს განცხადებას.

მტკიცება ფორმალურია და ნაშრომი დაშვებებს აშკარად ასახელებს. ეს დაშვებები შემთხვევითი არ არის. არაინტერაქტიული მოწმის განურჩეველი მტკიცებულებები კრიპტოგრაფიაში სტანდარტული ობიექტებია და რამდენიმე დამკვიდრებული დაშვების პაკეტიდან გამომდინარეობს. ოპტიმალური მტკიცებულებათა სისტემის არარსებობის ჰიპოთეზა მტკიცებულებათა სირთულის ცენტრალური ღია ვარაუდია. P = BPP კი სტანდარტული დერანდომიზაციის ჰიპოთეზაა და მხოლოდ ფალსიფიცირებადი თვისებების უფრო ფართო თეორემისთვის გამოიყენება.

ნაშრომი ასევე ამტკიცებს, რომ ეს დაშვებები შესაბამისი ფასია და არა თვითნებური საყრდენი: საპირისპირო მიმართულებასაც აჩვენებს და ამტკიცებს, რომ ისინი არსებითად აუცილებელია — თუ ასეთი კონსტრუქციები საერთოდ არსებობს, მაშინ არაინტერაქტიული მოწმის განურჩეველი მტკიცებულებები უნდა არსებობდეს და (სტანდარტული ცალმხრივი ფუნქციების არსებობის დაშვებით) ოპტიმალური მტკიცებულებათა სისტემა არ უნდა არსებობდეს. ეს „ორივე შემთხვევაში მომგებიანი“ ტიპის დაშვებებიცაა:

რომელიმეს უარყოფა თავისთავად მნიშვნელოვანი აღმოჩენა იქნებოდა მტკიცებულებათა სირთულეში, კრიპტოგრაფიაში ან სირთულის თეორიაში.

მაგრამ რადგან შედეგი პირობითია, მის მიმართ ნდობაც პირობითია. თუ ეს დაშვებები მცდარია, თეორემის ინტერპრეტაციაც იცვლება. და მათ ჭეშმარიტებად მიღების შემთხვევაშიც გარანტია სრული კლასიკური ნულოვანი ცოდნა არ არის; ეს ნაშრომის უფრო სუსტი, დამტკიცების თეორიული ვერსიაა.

ამიტომ შესაბამისი ნდობა ასეთია: მაღალი — რომ ნაშრომი თანმიმდევრულ პირობით შესაძლებლობის შედეგს ადგენს; საშუალო — რომ მისი დაშვებები აღწერს იმ კრიპტოგრაფიულ სამყაროს, რომელშიც რეალურად ვცხოვრობთ; და დაბალი — ნებისმიერი დაუყოვნებელი პრაქტიკული შედეგისთვის.

რატომ აქვს მნიშვნელობა

ნაშრომი ხსნის გზას, რომელიც თითქოს დახურული უნდა ყოფილიყო.

კლასიკური თეორია ამბობს: სრული ნულოვანი ცოდნა სქემის გარეშე ერთ შეტყობინებაში ვერ ჩაეტევა და სრული სისწორის გარანტია ვერ ექნება. ილანგოს ნაშრომი ამბობს: თუ ნულოვანი ცოდნის იმ შედეგებს მოვითხოვთ, რომელთა შემოწმებაც უსაფრთხოების თამაშებში შეიძლება, და თუ უსაფრთხოების განსაზღვრებას დავაკავშირებთ იმასთან, რისი ეფექტურად უარყოფა შეუძლია ან არ შეუძლია არჩეულ წესთა წიგნს, სასარგებლო ქცევის დიდი ნაწილი მაინც შეიძლება აღვადგინოთ — ერთი შეტყობინებით, სქემის გარეშე და სრული სისწორის გარანტიით.

ეს მცირე ტერმინოლოგიური კორექტირება არ არის. ეს კრიპტოგრაფიულ გარანტიებზე ფიქრის განსხვავებული გზაა. მხოლოდ იმას კი ნუ ვკითხავთ, რა არსებობს; ვკითხოთ, რისი გამორიცხვა შეუძლია ჩვენს ფორმალურ სისტემას. დაუმტკიცებლობას ფილოსოფიურ უსიამოვნებად კი ნუ მივიჩნევთ — გამოვიყენოთ ის სტრუქტურად.

პრაქტიკული სამყარო ხვალვე შეიძლება არ შეიცვალოს. მაგრამ კონცეპტუალური რუკა უკვე იცვლება. ახლა არსებობს ფორმალური აზრი, რომელშიც „ვერავინ შეძლებს ეფექტურად დაამტკიცოს, რომ საიდუმლო გაჟონა“ შეიძლება საკმარისად ძლიერი აღმოჩნდეს იმისთვის, რომ აღადგინოს ბევრი თამაშზე დაფუძნებული დაცვა, რომელსაც „საიდუმლო არ გაჟონილა“-სგან ველოდით.

სწორედ ამიტომ არის გიოდელი სათაურში.

მოკლე შეჯამება

ნულოვანი ცოდნის მტკიცებულებები საშუალებას აძლევს დამმტკიცებელს, შემმოწმებელი დაარწმუნოს განცხადების ჭეშმარიტებაში მოწმის გამჟღავნების გარეშე. კლასიკური შეუძლებლობის შედეგები ამბობს, რომ ნულოვანი ცოდნა სქემის გარეშე ერთ

შეტყობინებაში ვერ ჩაიტევა და სრული სისწორის გარანტია ვერ ექნება. რაჰულ ილანგოს ნაშრომი ამ შეუძლებლობებს არ უარყოფს. ის უფრო სუსტ ცნებას — ეფექტურ ნულოვან ცოდნას — განსაზღვრავს: იმის მოთხოვნის ნაცვლად, რომ სიმულატორი რეალურად არსებობდეს, მოითხოვება, რომ არჩეულმა მტკიცებულებათა სისტემამ — ZFC-ის მსგავსმა ფორმალურმა წესთა წიგნმა — ვერ შეძლოს ეფექტურად დაამტკიცოს, რომ სიმულატორი არ არსებობს. კრიპტოგრაფიის (არაინტერაქტიული მოწმის განურჩეველი მტკიცებულებები) და მტკიცებულებათა სირთულის (ოპტიმალური მტკიცებულებათა სისტემა არ არსებობს) მნიშვნელოვან დაშვებებზე დაყრდნობით, ნაშრომი NP/SAT-ისთვის აგებს ერთშეტყობინებიან დამმტკიცებლებს სქემის გარეშე და სრული სისწორის გარანტიით, რომლებიც ნულოვანი ცოდნის ფალსიფიცირებად, თამაშზე დაფუძნებულ შედეგებს თითო თვისების მიხედვით აღწევს. ერთი დამმტკიცებელი, რომელიც ყველა „ბუნებრივ“ ასეთ თვისებას მოიცავს, უფრო შორს მიმავალი და ნაწილობრივ ჰიპოთეზური გაფართოებაა — ხოლო ფაქტობრივად ყველა ფალსიფიცირებადი თვისების ერთდროულად დაფარვა სავარაუდოდ შეუძლებელია, რადგან მტკიცებულებები ხელახლა გამოყენებადია. შედეგი თეორიული და პირობითია, არა დანერგილი კრიპტოგრაფიული ინსტრუმენტი, მაგრამ აჩვენებს მტკიცებულებათა თეორიული დაუმტკიცებლობის კრიპტოგრაფიულ რესურსად გამოყენების ახალ გზას.

პირდაპირი შემოწმება

რას აჩვენებს ნაშრომი: მითითებული დაშვებების პირობებში შესაძლებელია NP/SAT-ის ერთშეტყობინებიანი, სქემის გარეშე, სრულყოფილი სისწორის მქონე დამმტკიცებლების აგება, რომლებიც ნებისმიერ წინასწარ არჩეულ მტკიცებულებათა სისტემასთან მიმართებით ეფექტურად ნულოვანი ცოდნაა და კლასიკური ნულოვანი ცოდნის თითოეულ ფალსიფიცირებად, თამაშზე დაფუძნებულ შედეგს აღწევს.

რა არის სავარაუდო, მაგრამ უპირობოდ დაუმტკიცებელი: რომ საჭირო მტკიცებულებათა სირთულისა და კრიპტოგრაფიული დაშვებები ჭეშმარიტია. ეს სერიოზული, კარგად შესწავლილი დაშვებებია — და ნაშრომი აჩვენებს, რომ ისინი არსებითად აუცილებელიცაა და საკმარისიც — მაგრამ მაინც დაშვებებია.

რას არ აჩვენებს: კლასიკურ ნულოვან ცოდნას ინტერაქციის გარეშე, სქემის გარეშე და სრული სისწორის გარანტიით; პრაქტიკულ, დანერგვისთვის მზად სისტემას; მტკიცებულებების უარყოფადობას ან ხელახლა გამოყენების შეუძლებლობას; ან იმას, რომ გიოდელის არასრულობის თეორემა თავისთავად კრიპტოგრაფიას იცავს.

მთავარი შეზღუდვები: გარანტია ნულოვანი ცოდნის მოდუნებული ვერსიაა; ყველაზე ფართო ფორმა რამდენიმე დაშვებას ეყრდნობა; ერთიანი უნივერსალური დამმტკიცებელის შესახებ მტკიცებები ნაწილობრივ conjectural რჩება; შედეგი კი პირველ რიგში საფუძვლით თეორიას ეხება.

რამდენად უნდა ენდოს ამას ზოგადი მკითხველი? მაღალი ნდობაა გამართლებული, რომ განსაზღვრებების მიღების შემთხვევაში ეს მნიშვნელოვანი პირობითი თეორიული შედეგია. საშუალო — რომ დაშვებები რეალობას აღწერს. დაბალი — დაუყოვნებელი

პრაქტიკული დანერგვისთვის. უსაფრთხო დასკვნა ასეთია: ნაშრომი ნულოვანი ცოდნის შეუძლებლობებს არ არღვევს; ის დამტკიცების თეორიული გზას პოულობს, რათა გვერდი აუაროს მათი იმ ნაწილების პრაქტიკულ შედეგებს, რომლებიც უსაფრთხოების მრავალ თამაშში მნიშვნელოვანია.

წყაროები

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