أنظمة للبرهنة الإحتمالية
(محاولة لتقديم نظرة عامة لغير المتخصصين)

Probabilistic Proof Systems
(an attempt at a presentation for the non-experts)

عوديد جولدرايخ، معهد وايزمان للعلوم
Oded Goldreich, Weizmann Institute of Science

عساف كفوري قام بترجمة النص من الإنجليزية إلى العربية
Assaf Kfoury translated the original English text to Arabic*

24 نوفمبر 2025

* يمكن تنزيل المقال الأصلي باللغة الإنجليزية من هذا الموقع على الإنترنت:
Probabilistic Proof Systems -- a popular exposition, intended for a general audience.

المحتويات

On typesetting and translating

There are several difficulties to consider when translating from English to Arabic.

The first difficulty is choosing a suitable text editor. When writing regular Arabic prose without science formalisms (of which mathematics is a part), there are many alternative systems, among which MS Word and LibreOffice are good and easy to use. However, when writing scientific documents, both of those systems are limited, in both English and Arabic. The standard system for typesetting scientific texts in English is LaTeX. Still, for typesetting in Arabic, LaTeX is also limited in what it offers, compared to the functions and features it provides for scientific texts in English. Despite these limitations, we have no alternative to LaTeX (and to compiling it with XeLaTeX).

Another difficulty, more open to different solutions and thus more time-consuming to solve, is how to translate long-established English concept names into Arabic. There are many different solutions for this difficulty because there is a far larger multiplicity of words suggesting the same meaning in Arabic than in English. Choosing an appropriate Arabic name for a concept long associated with a single English name is however only part of the difficulty.

The biggest difficulty lies in reconciling different Arabic names for a same concept when these names are the result of translations by different Arab scientists. Arabic-speaking scientists work largely in isolation from each other and are better connected in their daily work with English-speaking colleagues. It is not that those colleagues are native English speakers, but simply that English is increasingly becoming the lingua franca of the sciences.

Finally, anyone who wishes to pursue research in a scientific field must be familiar with the English names of its concepts. To facilitate the reader's transition between Arabic and English, we added English names and phrases after their Arabic translations in many places in the text. For further convenience, all technical words with their Arabic translations are in a glossary at the end of the article.

حول التنضيد والترجمة

هناك عدة صعوبات التي يجب مراعاتها في الترجمة من الإنجليزية إلى العربية.

الصعوبة الأولى تتعلق باختيار محرر نصوص مناسب. عند كتابة النثر العربي العادي دون صيغ ونصوص ومصطلحات علمية (والتي تُعد الرياضيات جزءًا منها)، فهناك العديد من الأنظمة البديلة، ومن بينها MS Word و LibreOffice هما نظامان جيدان وسهلان في الاستخدام. ولكن عند كتابة تقارير ومقالات علمية، فإن كلا النظامين محدودان إلى حد ما، سواء باللغة الإنجليزية أو باللغة العربية. النظام القياسي لتنضيد النصوص العلمية باللغة الإنجليزية هو LaTeX، ولكن بالنسبة للتنضيد باللغة العربية، فإن LaTeX محدود أيضًا فيما يقدّمه مقارنة بالعديد من الوظائف والميزات التي يوفّرها لإعداد النصوص العلمية باللغة الإنجليزية. وعلى الرغم من هذه النقائص ، ليس لدينا بديل لـ LaTeX (ولتجميعه باستخدام XeLaTeX).

هناك صعوبة أخرى، أكثر تعرّضًا لحلول بديلة من الصعوبة الأولى وبالتالي أكثر استهلاكًا للوقت في إيجاد حل لها، وهي كيفية ترجمة كلمات إنجليزية راسخة في تسميتها لمفاهيم علمية منذ عقود. وإذا كان هناك العديد من الحلول البديلة لهذه الصعوبة، فذلك لأن هناك تعددًا أكبر بكثير من الكلمات التي تشير إلى نفس المعنى في اللغة العربية مقارنة باللغة الإنجليزية. ومع ذلك، فإن اختيار اسم عربي مناسب لمفهوم مرتبط منذ فترة طويلة باسم إنجليزي واحد ليس سوى جزء من هذه الصعوبة.

لكن الصعوبة الأكبر تكمن في التوفيق بين الأسماء العربية المختلفة لمفهوم واحد عندما تكون هذه الأسماء نتيجة ترجمات قام بها علماء عرب مختلفون في السابق. يعمل العلماء الناطقون بالعربية إلى حد كبير في عزلة عن بعضهم البعض وعادة ما يكونون أكثر ارتباطًا في عملهم اليومي بزملاء ناطقين بالإنجليزية. ليس الأمر أن هؤلاء الزملاء هم من الناطقين بالإنجليزية كلغة أم، ولكن الواقع اليوم أن اللغة الإنجليزية أصبحت بشكل متزايد لغة مشتركة للعلوم وللباحثين العلميين.

وأخيرًا، فإن كل من يرغب في مواصلة الدراسة والأبحاث في أيّ مجال علمي لابد وأن يكون على علم بالأسماء الإنجليزية لمفاهيم هذا المجال. لتسهيل انتقال القارئ من العربية إلى الإنجليزية وبالعكس ، أدرجنا العديد من الأسماء والعبارات الإنجليزية مع ترجماتها العربية في مواقع مختلفة من النص. ولمزيد من التسهيل ، جمعنا أيضًا كافة الكلمات التقنية مع ترجماتها العربية في مسرد منفصل في نهاية هذا المقال.

موجز

يتم تعريف المفهوم التقليدي لأنظمة البرهنة ، وبالتحديد أنظمة البرهنة المسماة " أنظمة البراهين NP " ، على أساس عمليات تحقق حتمية. غير أن استعدادنا للانحراف عن أساليب البرهنة التقليدية والاعتماد على عمليات تحقق عشوائية واحتمالية يسمح بالعديد من الفوائد، بما في ذلك:

- تتميز أنظمة البرهنة التفاعلية، التي تستخدم أساليب تحقق عشوائية، بقدرة تعبيرية أكبر وقدرة استدلالية أكبر من أنظمة البرهنة التقليدية التي هي حتمية وغير إحتمالية (من نوع NP) ، وتؤكد على فوائد التفاعل والتبادل مقارنةً بالتواصل أحادي الاتجاه الذي يميز أنظمة البرهنة التقليدية.
- تتيح هذه الأساليب العشوائية في أنظمة البرهنة إدخال براهين صفرية المعرفة (zero-knowledge proofs) ، أي أنها غير كاشفة لأي معلومات ، وهي ذات أهمية نظرية وعملية كبيرة. تُظهر أنظمة البرهنة الاحتمالية هذه إمكانية فصل الإثبات عن التعلم (أي إمكانية إثبات ادعاء دون الكشف عن أي شيء يتجاوز صحته).
- يمكن تحويل البراهين التي تسمى NP بشكل موجز وفعال إلى ما يسمى بالبراهين القابلة للتحقق احتماليًا (probabilistically checkable proofs) والتي توفر توازناً بين عدد المواقع التي تم فحصها في برهان NP والثقة في صحته.

في جميع أنواع الأنظمة للبرهنة الإحتمالية المذكورة أعلاه، يجب فرض حدود واضحة على التعقّد الحوسبي (أو ما يسمى أيضًا بالتعقيد الحسابي) لعملية التحقّق، وهذا بدوره يفترض وجود مُحقِّق (ويسمى أيضًا مُتحقِّق) مسؤول عن تحديد هذه الحدود. علاوة على ذلك، بإمكان المحقق في جميع أنظمة البرهنة الإحتمالية هذه برمي عملة معدنية تكراراً (لتسجيل وجه أو ظهر هذه العملة بعد كل رمية) وبإتخاذ قرارات بناءً على الأدلة الإحصائية.[1] وبالتالي، تحمل جميع أنظمة البرهنة هذه احتمالية خطأ؛ إلا أن هذا الاحتمال مُحدد بشكل واضح وصراحةً ويمكن تقليله من خلال استخدام نظام البرهنة مجدداً وبشكل متكرر.

Abstract

[1] عملة معدنية عادلة هي تلك التي يكون احتمال وقوعها بعد كل رمية على أي من الجانبين (الوجه أو الظهر) متساويًا، أي أن هذا الاحتمال هو 1/2 لكل من الجانبين.

1 طبيعة القضايا التي سيتم مناقشتها Nature of the claims to be discussed

دعوني أبدأ ببعض الملاحظات التوجيهية. أولًا ، البراهين التي سأناقشها هي براهين (دقيقة) لقضايا قائمة بحد ذاتها ومكتفية ذاتياً. أي أن جميع المعلومات الكافية للتحقق من صحة قضية ما موجودة (ضمنيًا على الأقل) في نص القضية ، وليست هناك حاجة للحصول على أية معلومات خارجية. ومع ذلك ، يمكن تعزيز وتسهيل عملية التحقق من خلال إضافة معلومات خارجية (تشير إلى محتويات القضية). على سبيل المثال ، لنفترض أن لدينا نظام معادلات بالشكل التالي، ودعونا ننظر إلى القضية أو الإفتراض الذي ينص بأن هذا النظام له حل يتكون من أعداد صحيحة غير سالبة:

$$\begin{aligned} x+y+z &= 2 \\ x-y &\geqslant 0 \\ 2y+z &\leqslant 2 \\ z &\leqslant 1 \end{aligned}$$

وبالطبع ، يمكنكم بسهولة التحقق بنفسكم من صحة هذا الإفتراض بأن نظام المعادلات أعلاه لديه حل من أعداد صحيحة غير سالبة. ولكن يجب عليكم الاعتراف بأنه من الأسهل التحقق من صحة هذا الإفتراض عندما يتم إعطاؤكم برهاناً بشكل حل لنظام المعادلات هذا ، وبالتحديد بشكل إستبدال للمتغيرات $\{x,y,z\}$ (على سبيل المثال $x=y=1,z=0$). هذا البرهان ، أي هذا الحل ، لا يظهر صراحةً وبشكل واضح في نص المعادلات ، ولكنه مدرج ضمناً فيه. وبالمثل ، يحتوي نظام معادلات من النوع المذكور أعلاه أيضًا على جميع المعلومات اللازمة للتحقق من صحة توكيد أو إفتراض ينص بعدم وجود حل للنظام . ومع ذلك ، يبدو التحقق من هذا الإفتراض السلبي أكثر صعوبة (على سبيل المثال ، لا يمكن أن يتكون البرهان ، أي الحل ، من تعيين واحد للمتغيرات كمثال مضاد للمعادلات).

سأستخدم أنظمة معادلات متعددة المتغيرات (ومعادلات متعددة) كأمثلة عملية في هذه النظرة العامة. يوضح المثال أعلاه أيضًا أن القضايا والفرضيات التي أناقشها هي قضايا وفرضيات عادية جداً ، وليست مبرهنات أساسية مثل مبرهنة فيثاغورس الشهيرة (Pythagorean Theorem) أو مبرهنة فيرما الأخيرة (Fermat's Last Theorem) .

دعوني أعلق بأن المثال السابق يمكن استخدامه لتوضيح الأنواع الثلاثة لأنظمة البرهنة التي سنتناولها لاحقًا. إن برهاناً تقليدياً من نوع NP لنظام معين من المعادلات يتم توفيره عن طريق تحديد حل للمعادلات كتخصيص أعداد صحيحة للمتغيرات. ولكن يبدو أنه لا يوجد برهان من نوع NP لقضية ينص على أن مثل هذا النظام من المعادلات ليس له حل ، ومع ذلك فإن أنظمة البرهنة التفاعلية (العشوائية) يمكنها القيام بهذه المهمة. علاوة على ذلك ، ليس من الواضح كيفية صياغة برهان لإثبات أن مثل هذا النظام من المعادلات لديه حل دون تقديم أي معلومات إضافية حول هذا الحل ، ومع ذلك تم إنشاء أنظمة البرهنة صفرية المعرفة للقيام بذلك المهمة بالضبط.

اعتذار: لا تسألوني ماذا ترمز إليه الحروف الغربية NP. إنها اختصار رديء ، وهو يعكس ضعف مهارات العلاقات العامة لدى مجتمع باحثي نظرية الحوسبة. نتيجة لذلك ، نادرًا ما يُنقل المحتوى الفكري الرائع لنظرية الحوسبة إلى غير المتخصصين ، ناهيك عن عامة الناس.[2] إن هذه النظرة العامة هي محاولة متواضعة من جانبي لتصحيح هذا الوضع المؤسف.

[2] إن ما هو واقع وعي الأشخاص بالتأثير الثوري لتكنولوجيا الحوسبة على مجتمعنا لا يتعارض مع حقيقة أن قلة ضئيلة منهم فقط على دراية بنظرية الحوسبة. هذا التناقض ليس مفاجئًا ، لأن الناس يبدون منبهرين بعجائب هذه التكنولوجيا لدرجة أنهم لا يتساءلون عن النظرية التي تقوم عليها. علاوة

ملاحظة للقراء المتقدمين: إذا كنت أصر على إيجاد حلول بشكل أعداد صحيحة غير سالبة لأنظمة المعادلات الخطية ، فذلك لأن في هذه الحالة حتى إيجاد حل لنظام معادلات خطية هي مسألة NP-كاملة . وبالتالي ، فإن ما يُوضَّح حول قابلية أنظمة المعادلات الخطية لحلول صحيحة غير سالبة ينطبق أيضًا على أي فئة أخرى من القضايا حول الصنف NP، أي على نحو مكافئ ، على أي قضايا قابلة لبراهين من نوع NP.

على ذلك ، يميل الناس إلى التفكير في الحوسبة من منظور ملموس واجهوه في مواجهتهم الأخيرة بدلاً من منظور عام وعلى المدى البعيد.

2 المفهوم التقليدي للبرهنة: أنظمة البراهين NP Traditional NP-proof systems

إن المجد المنسوب عادة إلى براعة اختراع البراهين يجعلنا ننسى أن إجراءات التحقق وتفاصيلها الأقل تمجيدًا الواردة فيها هي التي تعطي البراهين قيمتها. في الواقع، من الناحية النظرية، تُعدّ معرفة وجود برهان ما مسألة ثانوية مقارنةً بإجراءات التحقق التي يُبنى عليها البرهان.

إن مفهوم إجراء التحقق يفترض مفهوم الحوسبة، بالإضافة إلى مفهوم الحوسبة الفعالة وجيدة الأداء. ويتجلى هذا الافتراض الضمني جليًا وواضحاً في أنظمة البرهنة من النوع NP ، حيث ترتبط الحوسبة الفعالة بالخوارزميات الحتمية التي يزداد وقت تشغيلها بشكل معتدل وبكمية محدودة مع طول بيانات الإدخال. (التعريف المعياري لدالة "متزايدة بشكل معتدل وبكمية محدودة" هو أنها تُعرَّف بدالة متعددة الحدود -- polynomial function.) ومن ثم ، تستخدم أنظمة البرهنة من نوع NP إجراءات تحقق فعّالة ذات الطول المعتدل في صياغتها مقارنةً بطول القضية الذي يتم إثباته.

إستطراد سريع: موضوع "P مقابل NP"

دعوني أبتعد قليلاً عن عرضي وأتساءل حول الاعتقاد الشائع بأن البراهين (أي البراهين من نوع NP) لها قيمة خاصة ولا ينبغي تجاهلها. أعتقد أن القراء يؤمنون بقيمة البراهين ، وأنا أعتقد ذلك أيضاً. ومع ذلك، فإن هذا الاعتقاد يرتكز على افتراض مفاده أنه من الأسهل التحقق من صحة برهان لقضية ما من تقييم صحة القضية بحد ذاتها عندما يتم تقديمها دون برهان. ولكن هل هذا الاعتقاد صحيح؟

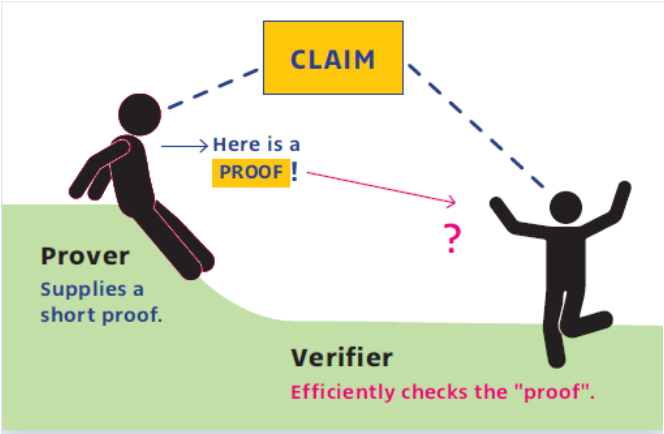
دعونا نفكر في المثال الجاري لنظام المعادلات والقضية بأن النظام له حل من أعداد صحيحة غير سالبة ، ولكن دعونا نفكر في الحالة التي يكون فيها النظام يحتوي على 100 معادلة في 100 متغير. يبدو من الصعب إن لم يكن من غير الممكن التحقق مما إذا كان مثل هذا النظام له حل صحيح غير سالب ، ولكن من السهل نسبيًا التحقق من صحة حل ما بمجرد تقديمه إلينا. ومن ثم، فإن مثل هذا الحل يُعد برهاناً (أي برهاناً من نوع NP) لصحة القضية بأن النظام لديه حل. **ولكن هل من الصعب ، إن لم يكن من المستحيل ، التحقق من وجود حل صحيح غير سالب لمثل هذا النظام (إذا لم يتم منحنا حلاً من أعداد صحيحة غير سالبة مسبقًا)؟**

والجواب على هذا السؤال هو أننا لا نعرف. هذا هو الموضوع الشهير المسمى "P مقابل NP" (بالإنكليزية "P versus NP"). الاعتقاد الشائع ، على الرغم من عدم وجود إثبات له ، هو أن الإجابة هي "نعم" ، أي أنه من الأسهل التحقق من صحة برهان لقضية ما من تقييم صحة القضية نفسها عندما يتم تقديمها دون برهان. إذا كانت الإجابة على هذا السؤال إجابة سلبية ، فإن ذلك يقوض مفهوم البرهنة ، لأن البراهين في هذه الحالة لا تقدم أي ميزة كبيرة في التحقق من صحة القضية. إن صحة هذا الاعتقاد الشائع هي بلا شك أهم مسألة مفتوحة في المعلوماتية النظرية.

العودة من الاستطراد: نظرة عن قرب على مفهوم أنظمة البرهنة

أذكركم أن العرض السابق لأنظمة البرهنة من نوع NP كان يشير إلى خوارزمية فعّالة واحدة، وهي الخوارزمية المسؤولة عن إجراء التحقق. دعوني أشرح متطلبات عملية التحقق، والتي تسمى **الاكتمال** و **السلامة.** تشير هذه المتطلبات إلى فئة من القضايا والمخمنات التي من المفترض أن يتعامل معها نظام البرهنة (على سبيل المثال، القضايا على وجود حل صحيح غير سالب لنظام المعادلات الخطية).

اكتمال: يتطلب هذا الشرط أن تكون للقضايا وللمخمنات الصحيحة (على سبيل المثال، فئة القضايا والمخمنات حول أنظمة



شكل 1: البراهين التقليدية: الاتصال أحادي الاتجاه. مُبرهِن = Prover ، مُحقِّق = Verifier .

المعادلات الخطية) براهين يتم قبولها (على أنها صحيحة) من خلال إجراء التحقق.

سلامة: يتطلب هذا الشرط ألا تكون للقضايا غير الصحيحة وللمخمنات غير الصحيحة (في الفئة) براهين مزعومة يتم قبولها (كما لو كانت صحيحة) من خلال إجراء التحقق.

إن هذين الشرطين بديهيان للغاية ، وأي نظام برهنة يجب أن يفترضهما: كلاهما معاً يؤكدان أنه من الممكن برهنة القضايا والمخمنات الصحيحة في النظام ، بينما لا يمكن برهنة القضايا والمخمنات غير الصحيحة فيه. دعونا ننظر إلى مثال القضايا التي تشير إلى أنظمة المعادلات الخطية. في هذه الحالة ، يشكل حل مقترح مكون من أعداد صحيحة غير سالبة برهاناً من نوع NP للقضية بأن نظام المعادلات الخطية له حل، حيث تتكون عملية التحقق من استبدال المتغيرات بالأعداد المقترحة ثم إجراء حساب التعبيرات الحسابية الناتجة.

أجدُ أنه من المفيد ، وخاصة في سياق ما يلي ، تقديم أنظمة البرهنة على أنها ألعاب بين طرفين ، بين **المحقق** (أو المُتحقق) الذي يستخدم عملية التحقق، و **المبرهن** الذي يزود المحقق ببراهين مزعومة. في الواقع ، فإن أي نظام برهنة يشير بوضوح إلى مهمة التحقق ، وهذه المهمة يجسدها المحقق ، ولكنه يشير أيضًا ضمناً إلى المبرهن باعتباره تجسيدًا لمصدر البراهين الممكنة والمفترضة.

بوجود هذا التجسيد أو التشخيص ، يمكننا أن نفكر في البراهين من نوع NP باعتبارها اتصالًا أحادي الاتجاه من المبرهن إلى المُحقق: يكتب المبرهن برهاناً مُفترضًا، ويقرأه المحقق ويتحقق منه (انظر **الشكل 1**).

يتطلب التشخيص السابق أيضًا تشخيصًا لشروط الاكتمال والسلامة: يعني الاكتمال أنه يمكن إقناع المُحقق بصحة القضية المطروحة من خلال براهين كافية ، والتي قد يقدمها المبرهن (الذي قد يكون أكثر دراية من المحقق) ، بينما تعني السلامة أنه لا يمكن لأحد خداع المُحقق بقبول برهان زائف لقضية مزيفة وغير صالحة . وبعبارة أخرى ، فإن الاكتمال يعني وجود استراتيجية (للمبرهن) لإقناع المحقق بالقضايا والمخمنات الصحيحة ، في حين أن السلامة تعني أنه لا يمكن لأحد إقناع المحقق بالقضايا والمخمنات المزيفة وغير الصحيحة.

كيفية تجاوز أنظمة البرهنة من نوع *NP*

الميزة الأساسية للبراهين من نوع NP ، والتي تعتبر أمراً مسلماً به ، هي أنها تستخدم إجراءات تحقق حتمية (أي عملية حوسبة يتم فيها تحديد كل خطوة بشكل فريد وبدون خيارات بديلة بناءً على الوضع والسياق الحالي). لقد ذكرتُ في المناقشة السابقة

أن إجراء التحقق هو عملية حتمية ، ولكنني أراهن على أن هذه الحقيقة لم يتم ملاحظتها من قبل القراء ، لأنه يؤخذ على أنها إفتراض قاطع ومسلم به عند مناقشة البرهنة العادية. أحد أسباب هذا الافتراض القاطع هو أن التحقق الاحتمالي يعني احتمالاً لحصول خطأ ، وهو ما يبدو متناقضًا مع المفهوم العادي للبرهنة. ولكنني أود دحض هذه الفكرة. على وجه الخصوص ، أود أن أؤكد على أن احتمال الخطأ سيكون محدودًا بشكل واضح وصريح ، وسيكون من الممكن تقليصه كما هو مرغوب فيه ضمن نطاق مناسب عن طريق التكرار وإعادة تطبيق نظام البرهنة مجدداً.

3 البرهنة التفاعلية (والعشوائية) Interactive (and randomized) proofs

إن النظر إلى برهان ما باعتباره لعبة أو تبادل بين طرفين ، بين محقق ومبرهن ، يعد أمراً أساسياً في تقديم أنظمة البرهنة التفاعلية. وبناءً على هذه النظرة ، فمن الطبيعي أن نفكر في أن التواصل سيكون ثنائياً الاتجاه أو مكوكياً (أي أنه سيكون تفاعلاً كاملاً بين المبرهن والمُحقق) بدلاً من أن يكون أحادياً الاتجاه (أي عندما يقتصر المبرهن على إرسال رسالة واحدة فقط إلى المُحقق وهذه الرسالة الواحدة تحتوي على مجمل البرهان المزعوم). ولذلك ستُسمى أنظمة البرهنة من هذه النوعية ، والتي تسمح بهذا النوع من الحوار والتبادل بين المبرهن والمُحقق ، بأنها أنظمة برهنة تفاعلية interactive proof (IP) systems (انظر **الشكل 2**). البراهين التفاعلية هي عمليات ديناميكية وليست كائنات ثابتة.

على الرغم من أن كلمة "العشوائية" لا تظهر في عبارة "البراهين التفاعلية" ، فمن السهل أن نرى أن العشوائية ضرورية لعملية البراهين التفاعلية مقارنةً بالبراهين من نوع NP. على النقيض من ذلك ، إذا كانت طريقة عمل المُحقق حتمية وغير عشوائية ، فيمكن للمُبرهِن أن يحدد مسبقًا جميع الخطوات التي يرسلها المُحقّق. في مثل هذه الحالة ، يمكن للمبرهن أن يقتصر على إرسال برهان واحد فقط من النوع NP يتضمن المحادثة بأكملها بين اللاعبين. الدرس العام هنا هو أنه لا جدوى من إجراء محادثة وتفاعل مع طرف يمكن التنبؤ بكل رسائله بسهولة. على النقيض من ذلك ، قد يكون التفاعل مع طرف آخر مفيدًا فقط إذا كان الطرف الآخر غير قابل للتنبؤ ورسائله غير معروفة مسبقًا (أي أنه يتصرف بشكل عشوائي) أو لديه المزيد من موارد الحوسبة (وبالتالي يمكنه القيام بعمل مفيد من أجلك).

ولكن ماذا عن المفاهيم الأساسية لأي نظام برهنة ، وبشكل خاص ، مفهوم الاكتمال ومفهوم السلامة ؟ عند استخدام استراتيجيات التحقق العشوائية والتفاعلية ، يجب تعديل هذه المفاهيم وصقلها لتعكس مفهومًا جديداً ومفيداً للأدلة ذات الطبيعة الإحصائية. على وجه التحديد ، في سياق أنظمة البرهنة التفاعلية ، يتم تعريف الاكتمال والسلامة على النحو التالي (فيما يتعلق باستراتيجية معينة يستخدمها المُحقق):

شرط اكتمال -- completeness condition: إذا كانت القضية أو المخمنة صحيحة ، فهناك استراتيجية بإمكان المبرهن أن يتبعها لجعل المحقق يقبل القضية أو المخمنة باحتمالية تساوي 1.

هناك أيضًا شرط اكتمال أضعف، أي أنه يتطلب أن يكون احتمال القبول $2/3$ على الأقل (وليس 1). في الواقع ، يمكن تحويل أنظمة من هذا النوع الأضعف إلى أنظمة من النوع القوي المذكور أعلاه.

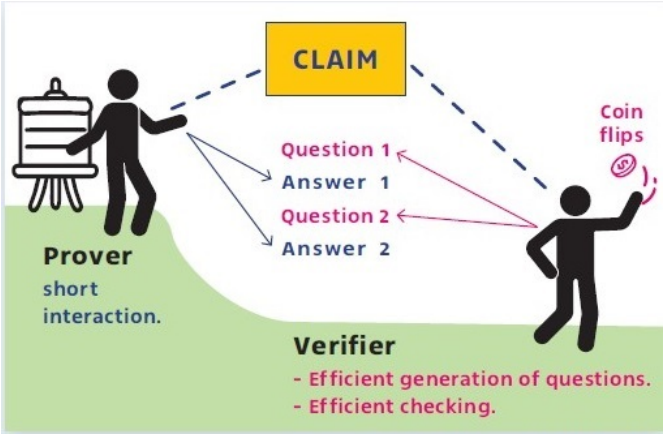
شرط سلامة -- soundness condition: إذا كانت القضية أو المخمنة غير صحيحة ، فإن أي استراتيجية يستخدمها المبرهن ستفشل في خداع المُحقق باحتمالية لا تقل عن $1/2$.

رغم أن الوقوع في فخ باحتمال $1/2$ هو أمر يصعب قبوله ، إلا أننا نستطيع خفض احتمال الوقوع في الفخ متى شئنا من خلال تفعيل النظام بشكل متكرر.

كما هو الحال في البراهين من نوع NP ، فإن شرط الاكتمال يفترض أنه يمكن برهنة القضايا والمخمنات الصحيحة في نظام برهنة تفاعلية ، وكما يفترض شرط السلامة أنه لا يمكن برهنة القضايا والمخمنات الخاطئة فيه.

مثال توضيحي: التماثل بين أنظمة المعادلات

يمكننا تعريف نظامين من المعادلات على أنهما متماثلان إذا كان بإمكاننا الانتقال من أحدهما إلى الآخر عن طريق تغيير أسماء



شكل 2: نظام برهنة تفاعلية = Interactive Proof (IP) system ،
مُبرهِن = Prover ، مُحقِّق = Verifier .

المتغيرات وتغيير ترتيب المعادلات .

لنفترض أن لديك نظامين من المعادلات ، كما في المثال السابق ، وتتساءل عما إذا كانا متماثلين ، أي أن تغيير أسماء المتغيرات وترتيب المعادلات في النظام الأول يُنتج النظام الثاني بالضبط . يمكن لبرهان من نوع NP الذي يُحدد استبدال المتغيرات وإعادة ترتيب المعادلات أن يُقنعك بسهولة بأن النظامين متماثلان . ولكن ماذا بالنسبة لإيجاد برهان بأن نظامي المعادلات ليسا متماثلين ؟ في الواقع ، لا نعلم ما إذا كانت هناك براهين من نوع NP لإثبات عدم التماثل بين نظامين من المعادلات الخطية ، ولكن هنا تأتي البراهين التفاعلية للإنقاذ.

ما يمكنك فعله كمُحقق هو اختيار أحد نظامي المعادلات عشوائيًا ، وإنشاء نسخة متماثلة عشوائية منه (عن طريق استبدال أسماء المتغيرات عشوائيًا وترتيب المعادلات عشوائيًا) ، وإرسال النتيجة إلى المبرهن ، طالبًا منه أن يُشير إلى مصدره (أي هل هو متماثل مع النظام الأول أو الثاني من المعادلات) . يُستوفى شرط السلامة لأنه إذا كانت أنظمة المعادلات مُتماثلة ، فلن يتمكن المبرهن من الحصول على الإجابة الصحيحة باحتمالية تتجاوز 1/2. من ناحية أخرى، يتم استيفاء شرط الاكتمال لأنه إذا لم تكن الأنظمة مُتماثلة ، فستكون نُسخها المُتماثلة أيضًا غير مُتماثلة.

النتيجة الإجمالية

استكمالاً للمثال السابق، لنتناول مسألة أكثر منطقية وأهمية لموضوعنا : التحقق مما إذا كان نظام المعادلات لا يحتوي على حلول من أعداد صحيحة غير سالبة. كما ذكرنا سابقاً ، يمكن استخدام البراهين من نوع NP لإثبات أن هذه الأنظمة لها حلول من النوع المذكور، ولكن يُعتقد على نطاق واسع أنه لا يمكن استخدام البراهين من نوع NP لإثبات أن هذه الأنظمة لا تحتوي على حلول من النوع المذكور. ومرة أخرى ، تأتي أنظمة البراهين التفاعلية للإنقاذ ، ولكنها معقدة للغاية بحيث لا يمكن عرضها هنا. دعوني أعيد صياغة النتيجة بشكل أوضح: **هناك براهين تفاعلية لإثبات أن نظام المعادلات ليس له حل من أعداد صحيحة غير سالبة .**

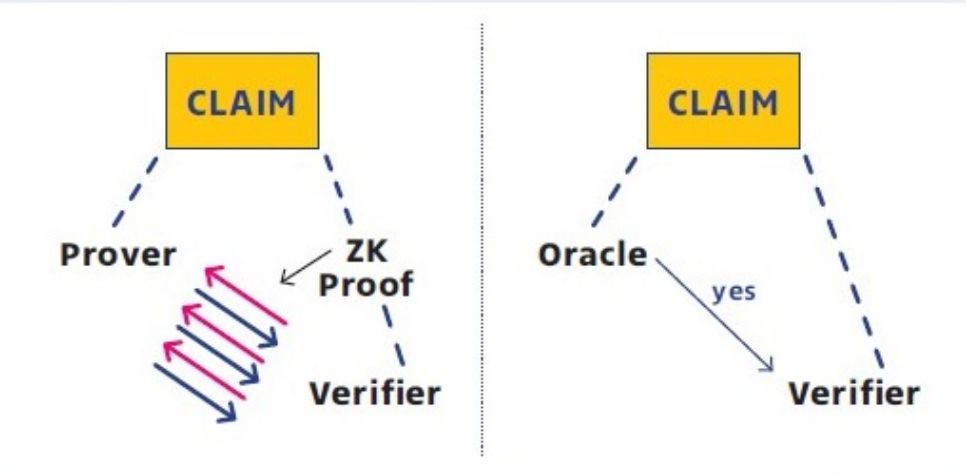
إجمالاً وبشكل عام ، لننظر في القضايا التي تُؤكد صلاحية "شيء" ما ، والتي تؤكدها ضمنيًا فقط في عباراتها ، ولنفترض أنه بمجرد تقديم هذا "الشيء" ، يُمكن التحقق من صلاحيته بسهولة . في مثالنا الحالي ، هذا "الشيء" هو حل من أعداد صحيحة غير سالبة لنظام المعادلات ، وهو موجود ضمنيًا في عبارات المعادلات . من الواضح أنه يُمكن استخدام برهان من نوع NP

لإثبات وجود "شيء" ذي أهمية في البيانات. اللافت للنظر هو أنه في هذه الحالة ، يمكن استخدام البراهين التفاعلية لإثبات عدم وجود ذلك الشيء في بيانات المعادلات . خلاصة القول هي أن البراهين من النوع NP كافية لإقناعنا بوجود "شيء" ما ، في حين يمكن استخدام البراهين من النوع IP لإقناعنا بأن نفس "الشيء" غير موجود.

ملاحظتان

في البرهان التفاعلي المُستخدم لإثبات عدم تماثل نظامي المعادلات ، كان من الضروري إخفاء الاختيارات العشوائية التي قام بها المُحقق عن المبرهن ، الذي لم يتلقَّ سوى تأثيرها على المُدخلات المشتركة لكلا الطرفين (المحقق والمبرهن) . وقد تبين لاحقًا أن هذا الاستخدام للعشوائية السرية كان غير ضروري ، بمعنى أن هناك نظام برهنة بديل لا يستخدم العشوائية السرية (والذي للأسف أكثر تعقيدًا في تعريفه وشرحه) . بشكل عام ، كل فئة من القضايا التي لديها نظام برهنة تفاعلية لديها أيضاً نظام برهنة يستخدم العشوائية الصريحة فقط . بعبارة أخرى ، في سياق وجود أنظمة برهنة من نوع IP ، لا توجد ميزة أو فائدة للأسئلة المعقدة (التي تخفي العشوائية) على الأسئلة العشوائية .

طوال المناقشة السابقة ، كان تركيزنا على تعقد مهمة المحقق ، وتجاهلنا تمامًا تعقد مهمة المبرهن . دراسة أكثر دقة تأخذ في الاعتبار تعقد كلتا المهمتين ، وتركز على أنظمة البرهنة التفاعلية التي لا تكون فيها البرهنة أصعب بكثير من اتخاذ القرار (بدون برهان) ، ويكون التحقق أسهل بكثير (من اتخاذ القرار). تُسمى أنظمة البرهنة التفاعلية هذه ، والتي لها أهمية عملية واضحة ، بالأنظمة ذات "الفعالية المضاعفة" (doubly-efficient) .



شكل 3: براهين صفرية المعرفة: العالم الحقيقي (على اليسار) مقابل العالم المثالي (على اليمين).
مُبرهِن = Prover ، مُحقِّق = Verifier ، برهان صفري المعرفة = ZK Proof ، إرشاد تَخَيُّلي = Oracle.

4 براهين صفرية المعرفة Zero-knowledge proofs

الانطباع الأساسي عن البراهين هو أنها تُعلّمنا المزيد عن الفرضية أو القضية التي نحن بصدد إثباتها من مجرد كونها صحيحة أو خاطئة . في الواقع ، عادةً ما تُقرأ البراهين وتُدرس لتعميق فهم القضية وسياقها وتداعياتها الأوسع . على النقيض من ذلك ، تُصمّم البراهين صفرية المعرفة بحيث لا تُعبّر عن أي شيء يتجاوز الصلاحية المجردة للقضية . من الواضح أن هذه سمة مُربكة وغير طبيعية ، ولا يُمكن أن توجد في سياق أنظمة البراهين من النوع NP. لذلك ، صُمِّمت في سياق أنظمة البراهين التفاعلية ، وهي سمة تُميّز البعض من هذه الأنظمة التفاعلية .

لنأخذ ، على سبيل المثال ، البرهان التفاعلي الذي استخدمناه لإثبات عدم وجود تماثل بين نظامين من المعادلات . في هذا البرهان ، لا يتعلم المُحقّق شيئًا من المُبَرهِن ، إذ يتحقّق فقط من أن إجابة المُبَرهِن تُطابق اختياره الأول (اختيار المُحقّق الأول) ، وهو ما يعرفه المُحقّق . الغرض الوحيد من هذا الاختبار هو التأكد من صلاحية الفرضية بأن الأنظمة (أنظمة المعادلات) المُعطاة ليست مُتماثلة.

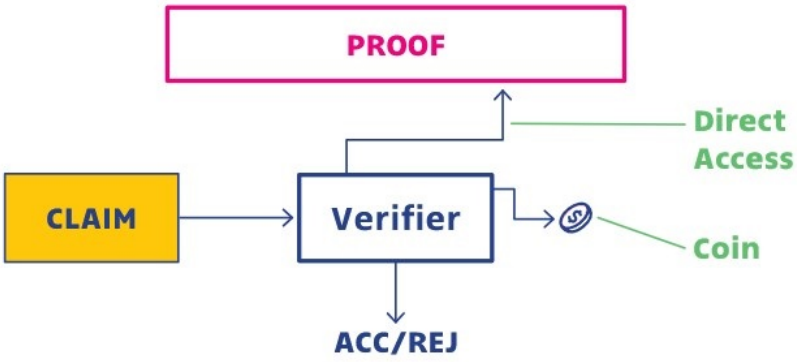
في هذه المرحلة ، يجدر بنا أن نتساءل كيف يُمكننا تعريف بدقّة العبارة التي تنص على أن "البرهان لا يكشف عن أي شيء يتجاوز صلاحية الفرضية أو صلاحية القضية" ، والتي استخدمناها لوصف وإعطاء فكرة حدسية عن مفهوم "البرهان صفري المعرفة وغير الكاشف عن تفاصيل عمليته الداخلية" . والجواب هو أن تعريف برهان صفري المعرفة من هذا النوع لقضية ما يُفسّر العبارة أعلاه على أنها تشترط أن أي شيء يُمكن استخلاصه بكفاءة من قبل المحقق بعد الحصول على تلك البرهان صفري المعرفة يُمكن استخلاصه بكفاءة أيضًا بناءً على نفس القضية من قبل المبرهن (بافتراض صحتها). بعبارة أخرى ، يُشير التعريف إلى عالمين مختلفين: العالم الحقيقي حيث تجري عملية البرهنة والبرهنة التفاعلية بين محقق ومبرهن ، وعالم مثالي حيث يُخبرنا طرف موثوق به وجدير بالثقة -- وسيط نعرفه بأنه "إرشاد تَخَيّلي" أو "مُرشد تَخَيّلي" (oracle) -- أن الفرضية صحيحة (انظر **الشكل 3**). يُشير التعريف إلى أن أي عملية إستخلاص يُمكن إجراؤها في العالم الحقيقي يُمكن إجراؤها أيضًا، بنفس الجهد تقريبًا، في العالم المثالي .

ومن ثم، فإن السبب الوحيد الذي يدفع المُحقق إلى الانخراط في برهان تفاعلي وصفري المعرفة هو الحصول على ضمان بأن القضية صحيحة ، وهو أمر كان سيكتسبه في عالم مثالي (غير موجود). وغني عن القول إن هذه الميزة الرائعة مفيدة جدًا في

نظرية التشفير (cryptography) ، حيث قد يرغب الأطراف في إثبات تصرفاتهم بشكل صحيح (وفقًا لأسرارهم) دون الكشف عن أي شيء عن أسرارهم .

دعونا نلقي نظرة أخرى على مثالنا لنظام المعادلات . في هذه الحالة ، إذا أكّد برهان صفري المعرفة بأن لنظام المعادلات يوجد حلّ من أعداد صحيحة غير سالبة ، فإنه لا يكشف عن أي معلومات داخلية حول هذا الحلّ ، حتى ولو كانت المعلومات جزئية . بل إنه فقط يُقنع المُحقق بوجود هذا الحل دون أية معلومة تدعم هذا الوجود . ومن المثير للدهشة أن برهاناً صفرياً المعرفة من هذا النوع تم اكتشافه حقاً وتصميمه لاحقًا ، بافتراض وجود ما يسمى بـ "الدوال أحادية الاتجاه" (one-way functions)، وهو افتراض ضروري لمعظم أنظمة التشفير الحديثة (وخاصةً لوجود أنظمة تشفير آمنة وتوقيعات رقمية (digital signatures) غير قابلة للتزوير).

بشكل عام ، كلما كان هناك نظام برهنة من نوع NP لفئة من القضايا (على سبيل المثال ، قابليّة أنظمة معادلات لحلول من أعداد صحيحة غير سالبة) ، فيوجد أيضًا نظام برهنة تفاعليّة وصفرية المعرفة لهذه الفئة . علاوة على ذلك ، يمكن جعل استراتيجيّة المُبرهِن ، في هذا البرهان التفاعلي وصفري المعرفة ، استراتيجيّة فعّالة ، بشرط أن يتمّ إعطاؤه برهان من نوع NP لإثبات القضية . (ضع في اعتبارك أن أي فئة من القضايا التي يمكن حلها بنظام برهنة تفاعليّة يمكن حلها أيضًا بنظام برهنة صفرية المعرفة .)



شكل 4: PCPs -- لدى المُحقق إمكانية الوصول المباشر إلى أجزاء من الإثبات.

5 براهين قابلة لتحقق احتمالي Probabilistically checkable proofs

دعونا الآن نعود إلى أنظمة البراهين من نوع NP التقليدية (أي ننسى أنظمة البراهين التفاعلية ونضعها جانباً) ، ولكن نستمر في اعتبار العشوائية جزءًا من عرضنا هنا .

إن شعورنا الأساسي تجاه البراهين التقليدية ، وخاصة البراهين من نوع NP ، هو أنه يجب قراءتها بالكامل. إن أولئك الذين يختارون تجاهل جزء من البرهان يخاطرون بقبول حجة خاطئة ، ما لم يعرفوا الجزء الذي تجاهلوه من مصدر آخر . على النقيض من ذلك ، فإن البراهين القابلة للتحقق احتماليًا ، والتي تسمى براهين من نوع PCP (وهذه الحروف الغربية إختصارٌ للعبارة Probabilistically Checkable Proofs) ، تسمح بتقييم صحتها من خلال قراءة أجزاء صغيرة منها (انظر الشكل 4). كما سيتم توضيحه لاحقًا ، يجب أن تكون هذه البراهين بشكل تكراري وعشوائي ، وأن يكون اختيار الأجزاء المراد قراءتها عشوائيًا .

لنأخذ ، على سبيل المثال ،الافتراض الذي ينص على أن نظامًا من المعادلات الخطية له حل متكون من أعداد صحيحة غير سالبة ، ولنأخذ أيضاً برهاناً من نوع NP الذي يتكون من أحد حلول هذا النظام . لا يمكن أن يكون هذا البرهان الذي هو من نوع NP برهاناً من نوع PCP أيضًا ، لأن نظام المعادلات قد يكون غير قابل لحل بسبب تناقض يتعلق بالقيمة المفروضة على أحد المتغيرات . هذا الواقع يشير إلى أن وجود برهان من نوع PCP لنظام المعادلات يجب أن يحتوي على التكرار ووفرة من المعلومات المكررة والزائدة عن الحاجة . وفيما يتعلق بضرورة إستخدام العشوائية ، تجدر الإشارة إلى أن التحقق الحتمي القائم على عدد قليل من المواضع في نظام المعادلات يعني أن برهاناً من نوع NP قصير جدًا في الواقع ، مما يتناقض مع المعتقدات الشائعة بشأن فئة المسائل من نوع NP .

إن الأفكار التي تقوم عليها عملية بناء البراهين من نوع PCP معقدة للغاية لدرجة أنني لا أستطيع شرحها في نطاق هذه المقالة . ولذلك سأكتفي باقتباس نتيجة مركزية في هذا المجال ، وهي أن أي برهان من نوع NP يمكن تحويله وترجمته بكفاءة إلى برهان من نوع PCP ، والذي هو بشكل زائد عن الحاجة (redundant) من حيث أن قراءة ثلاثة بتات (bits) منه توفر خصائص الاكتمال والسلامة . على وجه الخصوص ، في البرهان من نوع PCP الناتج ، يقرأ المُحقق ثلاثة بتات عشوائية فقط ومن ثم يرفض باحتمالية لا تقل عن 0.49 أي "برهان زائف" لأي فرضية زائفة ، بينما يقبل باحتمالية 1 برهاناً (مترجمًا كما هو مذكور أعلاه) لفرضية صحيحة .

دعوني أذكر أن قراءة ثلاثة بتات ولا تقل عن ذلك في برهان هو الحد الأدنى الذي يوفر خصائص الاكتمال والسلامة معنى، وأن حد احتمال الرفض البالغ 0.49 (الذي يمثل أي عدد ثابت أصغر من 1/2) هو أيضًا الأمثل (فيما يتعلق بقراءة ثلاثة بتات).

وفي الختام ، أودّ أن أشير إلى أن بناء أنظمة برهنة من نوع PCP كان له تأثير كبير على دراسة ما يسمّى بمسائل التقريب (approximation problems). وهذا هو الحال لأن عمليّة تقييم أو تقدير احتمال قبول محقّق لقضية معيّنة هي مسألة إستمثال (optimization problem) ، ويمكن اختزالها إلى العديد من مسائل إستمثال طبيعيّة أخرى . (قد يتطلب فهم هذا الارتباط بنظرية الإستمثال الإلمام بنظرية المسائل NP- تامة (theory of NP-completeness) ، حيث يلعب مفهوم الاختزال دورًا أساسيًا ومحوريًا.)

6 ثناء ، تقدير ، مراجع Credit and bibliography

لقد تجنبتُ عمدًا ذكر أسماء الباحثين الذين يستحقون أكبر قدر من التقدير بالنسبة إلى النظرية التي استعرضناها بإيجاز في هذا العرض. فهذه التقديرات ، وهي ضرورية في المقالات العلمية ، لا تُضيف شيئًا يُذكر لعامة الناس. علاوة على ذلك ، فإن ذكر أسماء قليلة يُنشئ فجوةً مصطنعة بين "المشاهير" المذكورين و"الباحثين العاديين" الذين يتم تجاهلهم. وهذا يتناقض مع الواقع الذي يُمثل فيه العلم مشروعًا جماعيًا.

لست على علم بأي مقالات أو تفسيرات جيدة تقدم مفاهيم نظرية الحوسبة بشكل عام ، ناهيك عن أنظمة البرهنة الاحتمالية ، لجمهور عام من غير المتخصصين. الكتب والاستطلاعات التالية (التي كتبتها) موجهة إلى طلاب البكالوريوس في المعلوماتية والرياضيات. وعلى وجه الخصوص ، تغطي المصادر [7, 6, 1] بالتفصيل الجزء الأكبر من المواد المقدمة في هذه النظرة العامة ، في حين تغطي المصادر [5, 4, 3, 2] الموضوعات التي تم ذكرها بإيجاز.

[1] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008.

[2] Oded Goldreich. *Foundations of Cryptography: Basic Tools*. USA: Cambridge University Press, 2001. ISBN: 0521791723.

[3] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. USA: Cambridge University Press, 2004. ISBN: 0521830842.

[4] Oded Goldreich. *Introduction to property testing*. English. 1st ed. United Kingdom: Cambridge University Press, Nov. 2017. ISBN: 9781107194052. DOI: 10.1017/9781108135252.

[5] Oded Goldreich. ``On Doubly-Efficient Interactive Proof Systems.'' In: *Foundations and Trends in Theoretical Computer Science* 13.3 (2018), pp. 158–246.

[6] Oded Goldreich. *P, NP, and NP-Completeness: The Basics of Computational Complexity*. 1st. USA: Cambridge University Press, 2010. ISBN: 0521122546.

[7] Oded Goldreich. ``Probabilistic Proof Systems: A Primer.'' In: *Foundations and Trends in Theoretical Computer Science* 3.1 (2007), pp. 1–91. ISSN: 1551-305X. DOI: 10.1561/0400000023. URL: http://dx.doi.org/10.1561/0400000023.

مسرد المصطلحات (مرتبة أبجديًا بالعربي) *Glossary (alphabetically ordered in Arabic)*

معادلات متعددة المتغيرات multivariable equations 3

معادلة ، معادلات equation, equations 3

مقدار ضئيل ، مقادير ضئيلة bit , bits (in the sense of very small quantities) 13

مقولة maxim, saying 13

موقع ، مواقع / موضع ، مواضع / مكان ، أماكن location, locations / position, positions / place, places 1

مُبَرْهِن prover 6

مُحَقّق / مُتَحَقّق verifier 6

مُخَمَّنة ، مخمنات conjecture, conjectures 5

نظام برهنة من نوع IP / برهان تفاعلي IP-proof system / interactive proof 8

نظام برهنة من نوع NP NP-proof system 2, 3, 5

نظام برهنة proof system 2

نظام معادلات خطية system of linear equations 3, 4

نظرية الحوسبة theory of computation 3, 15

يُستوفى الشرط / يتم استيفاء الشرط the condition is satisfied / met 9