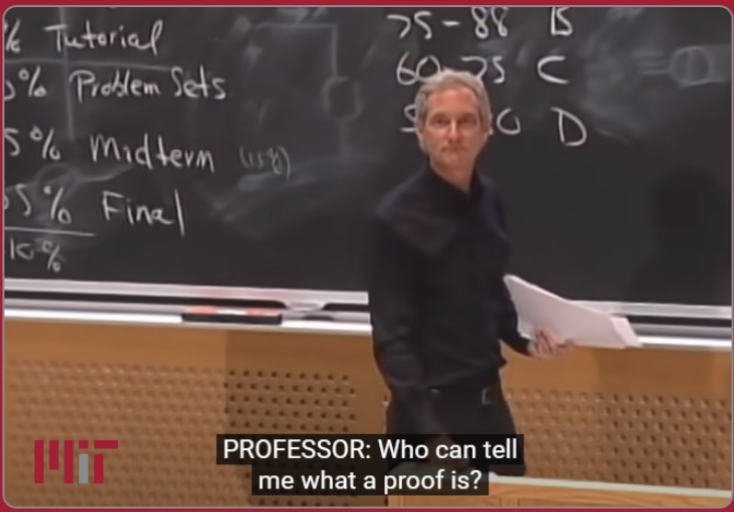

Lec 1 | MIT 6.042J Mathematics for Computer Science, Fall 2010
Instructor: Tom Leighton
Book: Mathematics for Computer Science

ملخص المحاضرة الأولي وأول شابتر من كورس وكتاب Mathematics for computer science لمعهد الـ MIT بعنوان Introduction and Proofs.

في البداية أيه هو الـ Proof؟ الـProof او البرهان هو طريقة للتحقق من حقيقة شيء ما او إثبات حقيقة شيء ما.في المجتمع في طرق كتير للتحقق من حقيقة شيء ما زي مثلا الملاحظة والتجربة، القضاة، الدين، رئيسك في الشغل، في مجال التجارة مثلا في مثل بيقول الزبون دايما على حق.

طيب ايه هو ال mathematical proof؟

a Mathematical proof is a verification of a proposition by a chain of logical deductions from a set of axioms.

خد بالك ان في التعريف ده في 3 حاجات مهمين جدا وهم اللي هتدور حواليهم المحاضرة دي وهم الـ proposition و logical deductions و axioms.

تعالى نبدأ بأول حاجه يعني ايه proposition ؟ ال proposition هي جملة يا أما تكون true او تكون false مثال على كده 2+3 = 5 ، دي statement اهي وقيمتها true، طيب 1 + 1 = 7 دي بردو statement ولكن false.

عندي حاجه تانية اسمها Predicate ودي بتكون عبارة عن statement لكن فيها متغير والـtruth value بتاعتها بتعتمد على المتغير ده معنى كده ان في طريقتين عشان احول الـpredicate دي لـ proposition يا أما اعوض عن المتغير بقيمة حقيقية ، او حاجه تانية اسمها quantification مثال على كده:

$\forall n \in N\ (n^2 + n + 41)$ is a prime number

حرف الـA المقلوب ده أسمه universal quantifier وبيتنطق كده for all يعني ترجمه الجملة اللي فوق دي: For every nonnegative integer, n, the value of $n^2 + n + 41$ is prime. والـN هنا اسمها universe of discourse.

معنى كده ان الstatement دي ترو لكل الأعداد الغير السالبة، وبالتالي عشان نقدر نثبت الكلام ده محتاجين نجرب كل الأرقام الغير سالبة! تعالى نجرب كده 0 هيطلعلك 41 وده فعلا عدد أولي، طب تعالى نجرب 1 هيطلعلك 43 وده بردو عدد أولي ،افضل جرب كده لحد 39 هتلاقي كل اللي هيطلعلك أعداد أولية، يعني شكل كده الstatement ده هتطلع صح ولا ايه! طب تعالى نجرب 40 كده، هيطلعلك 1681 بس ده مش عدد أولي! إذا بما ان الـstatement اللي فوق دي بتقول ان المعادلة دي true لكل الأعداد الغير سالبة وانت لقيت عدد الـstatement عنده بـfalse إذا الجملة دي غير صحيحة والرقم اللي انت لقيته اللي اسمه 40 ده بيسموه counter example.

مثال آخر:

$a^4 + b^4 + c^4 = d^4$ has no solution when a; b; c; d are positive integers.

بيقولك من الأخر كده مستحيل تلاقي 4 ارقام غير سالبة تحقق العلاقة دي، وده كان conjecture من Euler في سنة 1769، وconjecture ده معناها انها statement لسا مقدرناش نعرف اذا كانت true ولا false يعني لا ترقي انها تكون theory لان منقدرش نجرب كل الأعداد الغير سالبة لان ملهاش نهاية وفي نفس الوقت لم نجد counter example ليها عشان نثبت انها خطأ، الكلام ده فضل قرنين لحد ما أخيرا حد قدر يـdisprove it ووجد فعلا counter example ليها وكانت الأرقام كده:
a = 95800 , b = 217519 , c = 414560 , 422481

مثال آخر :
$313(x^3+y^3) = z^3$ has no solution when $x; y; z \in Z^+$

مش عايز أفاجئك بس اول counter example وجدوه كان رقم بيحتوي على اكتر من ألف digits! نيجي بقى للسؤال المهم، وأنا أيه اللي يخليني احاول الاقي حلول لحاجات زي دي؟ وليه في ناس ممكن تقضي وقت كبير جدا من حياتها في محاولة إيجاد حلول لحاجات زي دي؟

- الموضوع ده مهم عشان ال factoring اللي هو الطريق عشان تقدر تكسر crypto systems زي RSA واللي هو بيستخدم في كل حاجه بتقوم بيها إلكترونيا النهاردة من الشراء أون لاين والـSSL وده كله معتمد على الـNumber theory وبالتحديد الـfactoring. أنت لو تقدر تكسر الـCrypto Systems اه مش هتحكم العالم بس هتكون قريب من كده :)

احنا شوفنا اكتر من مثال لحد دلوقتي وكل واحد فيهم له حل، لكن في حاجات حتى النهاردة ملهاش حل، مثلا goldbach conjecture ، بيقولك ان اي رقم موجب زوجي معادا الـ2 تقدر تمثله عن طريق جمع عددين أوليين الكلام ده من 1742 لحد النهاردة محدش قدر يعرف اذا كانت true او false! ودي مصنفة كواحدة من أعظم الألغاز الغير محلولة على الإطلاق.

في نوع مهم جدا من الـstatements وهيكون مبني عليها حاجات كتير بعد كده وهي ال conditional statement واللي هي على الشكل ده : افترض ان عندك أتنين propositions وليكن p, q، الـstatement بتاعتك بتكون على الشكل ده If p, then q وبالرموز هتكون كده $p \rightarrow q$ والـ statement دي بتكون false في حالة واحدة فقط وهي لو الـp قيمتها true والـq قيمتها false. يعني لو عملت truth table فدي الحالة الوحيدة بس اللي هيكون فيها $p \rightarrow q$ بـfalse.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

الحاجة التانية اللي كانت في اول تعريف اخدناه الخاص بالـmathematical proofs وهي الـ Axioms ودي عبارة عن propositions بردو لكن احنا بنفترض انها true ملهاش إثبات يعني، حاجه انت شايفها منطقية جدا عشان تفترض انها true ، على سبيل المثال a = b , b = c أذا a = c ، وخد بالك ان في ناس بتقول ان في الرياضيات مينفعش تعمل إفتراضات وده كلام غلط طبعا لازم تبدأ بإفتراضات وإلا مش هتقدر توصل لحاجة أساسا. حاجه مهمة انك تحدد الـaxioms بتاعتك عشان اي حد بيقرأ ال proof بتاعك يشوفها وبالتالي لو هو متفق مع الـaxioms دي فهيتفق مع الـ conclusion.

تالت حاجه والأخيرة في التعريف وهي الـ Logical Deductions او الـ Rules of inference ودي بستخدمتها عشان اثبت propositions جديدة بإستخدام proposition انا أثبتها قبل كده، يعني تعالى كده على سبيل المثال نمسك الـ conditional statement اللي اتكلمنا عنها فوق:

لو قولتلك ان عندك proposition اسمها p وقيمتها true وقولتلك ان عندك $p \rightarrow q$ كمان true تقدر تستنتج ايه من الكلام ده ؟ الإستنتاج ان الـq كمان true ، طب ازاي؟ لان احنا قولنا فوق ان الحالة الوحيدة ان $p \rightarrow q$ تكون بـfalse وهي لو الp ترو والq بfalse بس هنا انا قولتلك ان $p \rightarrow q$ بtrue وبالتالي الq مستحيل تكون false فإذا لازم تكون true.

مثال تاني لو قولتلك ان الproposition دي p and q ترو ، يبقى إذا تقدر تستنتج ان الـp بترو والـq كمان بترو.

تقدر تبحث عن باقي ال Rules of inference على جوجل.

وبكده ده يكون ملخص المحاضرة الأولى والشابتر الأول في الكتاب الخاص بالـMIT

أتمنى يكون مفيد، مع تحياتي: محمد صلاح.

https://www.linkedin.com/in/mohamed-salah-039b35109