probabilistic proof

Canonical name	ProbabilisticProof
Date of creation	2013-03-22 15:53:44
Last modified on	2013-03-22 15:53:44
Owner	Algeboy (12884)
Last modified by	Algeboy (12884)
Numerical id	9
Author	Algeboy (12884)
Entry type	Example
Classification	msc 00A35

Most exciting results in mathematics make use of standard proofs; however, some emerging mathematics is making use of proofs nearly as exciting as the results. One of these methods in the Probabilistic method. The following is an outline of how such a proof might proceed.

Theorem structure:

Let X be a finite family of objects. We wish to show every element of X has some property T.

Proof scheme:

(i) Show that the probability that an object A in X has the property T is $1-\varepsilon$ for some $0 \leq \varepsilon \leq 1$.

(ii) Suppose $A \in X$ is some object without property T. Use A to construct more than $\varepsilon|X|$ other objects in X also without property T.

(iii) Conclude that if an object $A \in X$ does not have property T then the probablity that a random element of X has property T is less than $1-\varepsilon$ thus creating a contradiction. So every element in X has property T.

(See Examples of probabilistic proofs.)

The surprising discovery is that in some problems it is possible to show both (i) and (ii) thus establishing the contradiction in (iii). One would typically expect that to demonstrate the probablity is $1-\epsilon$ would necesitate knowing that there are no more than ϵ counterexamples, but this is not always the case.

Proofs of this flavor appear in graph theory because of a wealth of knowledge about random graphs and random walks etc. (Example, the work of Alon on H-universal graphs.) Establishing the necessary probabilities is therefore possible without carefully enumerating the elements in X. Then beginning with a possible counterexample, combinatorial changes are made to the candidate to create too many counterexamples.

A second technique applies to the mathematics of logic, more explicitly model theory. Recent work by Marcus du Sautoy treats problems on counting the number of p-groups through model theory.

Both proof techniques are highly non-constructive and can leave a reader wondering if they trust the result, but each is as foundational as a proof by induction.