Probabilistic Verification of Elementary Geometry Statements*

Giuseppa Carrà Ferro
Dip. di Matematica
Universitá di Catania
carra@dipmat.unict.it

Giovanni Gallo
Dip. di Matematica
Universitá di Catania
gallo@dipmat.unict.it

Rosario Gennaro
Lab. for Computer Science
M.I.T.
rosario@lcs.mit.edu

April 6, 1995

One of the very first principle that we all learn in High School while approaching Euclid's Geometry is: 'Examples teach us nothing'. In reality, for most Geometry theorems, examples provide the bases to conjecture a statement and encourage the learner to look for a rigourous proof of it. In this presentation we address the question: *How much should we trust an example?* A way to answer quantitatively such a question is to use the language of probability. The question could be hence reformulated in *What is the probability that a property verified for N examples is a theorem?*

In 1980 J.T.Schwartz in a now classical paper answered an analogous question about polynomial identities: *If two polynomials agree on a set of N points what is the probability that they are identical?*

Wu's procedure to prove geometrical statements provide a quick way to transfer Schwartz' results to the above question. Indeed the truth (or, better, the generic truth) of a statement turns out, in Wu's formulation, to be equivalent to the vanishing of a polynomial. If an example verifies a given statement, it corresponds to a zero of a certain polynomial. In presence of a large enough number of such positive examples (or, equivalently, of a large enough number of zeroes of the polynomial) it is possible to estimate the probability that the theorem is generically true.

The idea sketched above is quite well known, by now, to the community of people interested to algebraic methods for theorem proving. We do not know, however, of any quantitative analysis similar to the one reported here. We use the bounds of Gallo and Mishra on the degree of Wu-Ritt's characteristic sets to give an accurate estimate of the probability that a given statement is a theorem after N positive examples have been observed.

Our results could be summarized as follows. Let $B = c_1 C^{c_2(C+P)^2}$ where c_i are constants and P, C denote respectively the number of points and the number of circle or straight line constructions in a statement of plane Euclidean Geometry. Let h be the number of

*Preliminary Abstract

indipendent parameters needed to completely specify an example. Let I be a set of $2B$ elements in an algebraically closed field k. Choose N examples by sampling N random points from I^h. If this N examples verify the statement, then, with probability greater than $1 - 2^{-N}$, the statement is generically true.

We make use of Wu's procedure to get a probability estimate but it should be observed that once the statement under consideration has been formalized in a set of polynomial equations our probabilistic estimate applies even when the verification of the examples is done with techniques other than Wu's.