ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ, 157 84 ΖΩΓΡΑΦΟΥ ΤΗΛ 210 - 72 76 407
FAX 210 - 72 76 417, mail: cchondro@math.uoa.gr

Διαπανεπιστημιακό-Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών στη Λογική και Θεωρία Αλγορίθμων και Υπολογισμού

# ΣΕΜΙΝΑΡΙΟ ΛΟΓΙΚΗΣ ΚΑΙ ΑΛΓΟΡΙΘΜΩΝ

**Ομιλητής:** Γ. Μοσχοβάκης, U.C.L.A. και Μ.Π.Λ.Α.

**Θέμα:** The Axiomatic Derivation Of Absolute Lower Bounds

**Ημερομηνία:** Παρασκευή, 22/10/2010, 18:15

**Αίθουσα:** Γ33, Τμήμα Μαθηματικών, Ε.Κ.Π.Α.

## Περίληψη

The ancient Euclidean algorithm computes the greatest common divisor $\gcd(m,n)$ of two natural numbers from (or *relative to*) the remainder operation rem, which is assumed as *primitive*; it requires no more than $2\log(\min(m,n))$ applications of the remainder operation to compute $\gcd(m,n)$ (for $m \geq n \geq 2$), and it is not known to be optimal:

Conjecture. *For every algorithm $\alpha$ which computes on $\mathbb{N}$ from* rem *the greatest common divisor function, there is a constant $r > 0$ such that for infinitely many pairs $a \geq b \geq 1$,*

$$c_\alpha(a,b) \geq r \log_2(a),$$

where $c_\alpha(m,n)$ counts the number of calls to "the remainder oracle" required by $\alpha$ for the computation of $\gcd(m,n)$. The conjecture claims a logarithmic worst-case lower bound for *all algorithms* which compute $\gcd(m,n)$ from the remainder operation, not just those expressed by a specific class of computation models.

In this lecture I will describe an approach to the theory of algorithms in the style of *abstract model theory* which makes it possible to make precise and (on occasion) prove the existence of non-trivial, absolute lower bounds for a wide variety of problems and specified primitives, including those in the the bibliography.

Note. Three years ago I gave a lecture in the MPLA Seminar with the exact, same title and an almost identical abstract; there are. however, a few new results in the area.

## References

[1] Lou Van den Dries and Yiannis N. Moschovakis. Is the Euclidean algorithm optimal among its peers? *Bulletin of Symbolic Logic*, 10:390–418, 2004.

[2] Lou Van den Dries and Yiannis N. Moschovakis. Arithmetic complexity. *ACM Trans. Comput. Logic*, 10(1):1–49, 2009.