Overview of "Algorithmic Learning Theory and Cryptography"

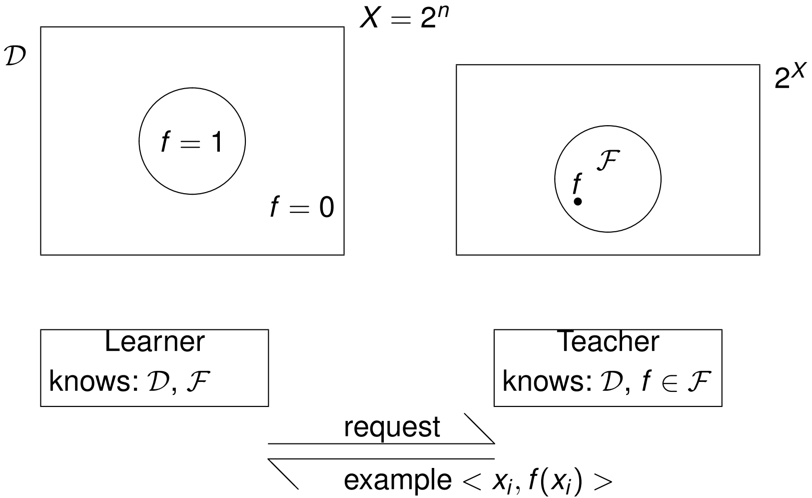
Tobias Eibach

Institute of Theoretical Computer Science
University of Ulm

25.4.2007

Outline

PAC LEARNING SCHEMA



Definition

An algorithm A learns a class of functions $\mathcal{F}$ if $\forall$ f $\in \mathcal{F}$ and ϵ, $\delta > 0$, the algorithm A outputs an hypothesis h with probability $1 - \delta$ such that

$$error(f, h) \leq \epsilon$$
$$error(f, h) := Pr_{x \in \mathcal{D}}[f(x) \neq h(x)]$$

The running time is polynomial if it's polynomial in n, $1/\epsilon$ and $log(1/\delta)$.

Main Lemma

Main Lemma

Let f be a Boolean function on n variables computable by a Boolean circuit of depth d and size M, and let t be any integer, then

$$\sum_{S \subset \{1..n\}, |S| \geq t} \hat{f}(S)^2 \leq M 2^{-t^{1/d}/20}$$

By N. Lineal, Y. Mansour and N. Nisan.

Main Lemma

The Main Lemma follows from the following 2 results:

Lemma (Hastad)

$$\Pr_{\rho}[\text{DT-depth}(f_{\rho}) \geq \text{s}] \leq \; M2^{-s}$$

Where ρ is a random restriction with parameter $p \leq \frac{1}{10^d s^{d-1}}$.

Lemma

$$\sum_{|S|>t} \hat{f}^2(S) \leq 2\Pr_{\rho}[\text{DT-depth}(f_{\rho}) \geq tp/2]$$

Learning AC^0

Corollary

Functions in AC^0 can be learned efficiently.

No pseudorandom function generators in AC^0

$f : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}$ is called PRFG if no oracle TM M running in polynomial time can distinguish between a truly random oracle and the oracle $f(s,*)$, s chosen at random.

Corollary

There exists no PRFG in AC^0.

A PRIVATE KEY CRYPTOSYSTEM

A private cryptosystem based on a non-learnable function class (on the average)

- natural mapping
- private key CS (G,E,D)
- first G generates a function f represented by σ
- D(E(m,σ),σ) = m
- encrypt 0 by a neg. example and 1 by a pos. example

REFERENCES

N. Lineal, Y. Mansour, N. Nisan.
Constant Depth Circuits, Fourier Transform, and Learnability.
Journal of the ACM, Vol. 40, No. 3, 1993, pp. 607-620.

A. Blum, M. Furst, M. Kearns, R. Lipton.
Cryptographic Primitives Based on Hard Learning Problems.
Lecture Notes in Computer Science, Vol. 773, 1994, pp. 278-291.

RESEARCH TOPICS

- Lower Bounds on Cryptographic Primitives
- Relationship between A.L. and Zero Knowledge
- Applications of Game Theory in Cryptography and Algorithmic Learning Theory
- Latest developements in A.L.T. (learning of juntas, sensitivity of monotone decision trees, noisetollerance learning, agnostic learning) and their influence in Cryptography.
- Implementation of Steganographic Tools

The End

Thank you!

(full talk: http://theorie.informatik.uni-ulm.de/Personen/eibach/)