# A THEORY OF THE LEARNABLE (L.G. VALIANT)

Theory Lunch Presentation
Claire Le Goues
05/20/10



## HOW DO YOU KNOW THAT?

#### HOW DO YOU KNOW THAT?

#### HOW DO YOU KNOW THAT?

## HOW DID YOU LEARN THAT?

"A program for performing a task [like recognizing ducks – Ed.] has been acquired by learning if it has been acquired by any means other than explicit programming."

 Present a general framework for reasoning about what is learnable as allowed by algorithmic complexity.

- Present a general framework for reasoning about what is learnable as allowed by algorithmic complexity.
- Introduce the idea of Probably Approximately Learnable (PAL) problems, or problems that are learnable in polynomial time, with high correctness.

- Present a general framework for reasoning about what is learnable as allowed by algorithmic complexity.
- Introduce the idea of Probably Approximately Learnable (PAL) problems, or problems that are learnable in polynomial time, with high correctness.
- Prove 3 classes of programs to be PAL.

#### Outline

- 1. General framework for defining Learning Machines, or programs that can learn/write/produce other programs of a particular type.
  - A Learning Machine for animal recognition, for example, might learn to write a program that recognizes whether a given animal is a duck.
- 2. Definition of a particular learning protocol.
- 3. Definition of when a program class is reasonably-learnable.
- 4. Definition/proofs of reasonably-learnable program classes.



 Focus on learning skills that involve recognizing whether a concept (boolean predicate) is true for given (boolean) data.

 Focus on learning skills that involve recognizing whether a concept (boolean predicate) is true for given (boolean) data.

 Learn to answer the question: is this animal a duck?

 Focus on learning skills that involve recognizing whether a concept (boolean predicate) is true for given (boolean) data.

 Learn to answer the question: is this animal a duck?

```
walks like a duck = true
   purple = false
   fluffy = true
   yellow = true
   beak = true
   big = false
quacks like a duck=true
   angry = false
...
```

+ Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:

- Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- \* A vector is an assignment to each of the t variables one of {0,1,\*}.
  - \* means "undetermined."

- Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- \* A vector is an assignment to each of the t variables one of {0,1,\*}.
  - \* means "undetermined."
- Function (concept) \( \mathcal{F} \) maps all vectors to \( \{0,1 \} \).
  - Learning machine is learning concepts.
  - The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

- Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- \* A vector is an assignment to each of the t variables one of {0,1,\*}.
  - \* means "undetermined."
- Function (concept) \( \mathcal{F} \) maps all vectors to \( \{0,1 \} \).
  - Learning machine is learning concepts.
  - The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

#### Low-

#### ions

+ Given t boo

o<sub>1</sub>,...,p<sub>t</sub>:

- + A vector is a each of the t variables one of {0,1,\*}.
  - \* means "undetermined."
- Function (concept) \( \mathcal{F} \) maps all vectors to \( \{0,1 \} \).
  - Learning machine is learning concepts.
  - The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

# Low-lion

- + Given t boo
- + A vector is a each of the

0<sub>1</sub>,..., p<sub>t</sub>:

- Variables: {walks like a duck, beak, purple, ...}
- Vector v: {walks\_like\_a\_duck=0, beak=1, purple=\*, ...}
- $+ F(v) = is_a_duck(v) = false$ 
  - to {U, 1}.
    - Learning machine is learning concepts.
    - The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

- Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- + A vector is an assignment to each of the
  - Variables: {purple, walks like a duck, beak, ...}
  - Vector v: {purple=\*, walks\_like\_a\_duck=0, beak=1 ...}

Variables determined in v: {walks\_like\_a\_duck, beak}

```
to {0,1}.
```

- Learning machine is learning concepts.
- The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

- Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- A vector is an assignment to each of the
  - Variables: {purple, walks like a duck, beak, ...}

Variables determined in is\_a\_duck: {walks\_like\_a\_duck, quacks\_like\_a\_duck}

- + Fu + F(v) = is\_a\_duck(v) = false

  to {U,1}.
  - Learning machine is learning concepts.
  - The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

- Given t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
   A vector is an assignment to each of the
   t boolean variables p<sub>1</sub>,..., p<sub>t</sub>
   Vectors assign variables to one of {0,1,\*}.
   FI Concept F maps vectors to {0,1}.
  - Learning machine is learning concepts.
  - The variables used in  $\mathcal{F}$  are determined in  $\mathcal{F}$ .

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- + Concept  $\mathcal{F}$  maps vectors to  $\{0,1\}$ .

```
    t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
    Vectors assign variables to one of {0,1,*}.
    Concept $\mathcal{F}$ maps vectors to {0,1}.
```

\* Assume  $\mathcal{D}$ , a probability distribution over all vectors  $\mathbf{v}$  which  $\mathcal{F}$  evaluates to 1.

```
    t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
    Vectors assign variables to one of {0,1,*}.
    Concept $\mathcal{F}$ maps vectors to {0,1}.
```

- \* Assume  $\mathcal{D}$ , a probability distribution over all vectors  $\mathbf{v}$  which  $\mathcal{F}$  evaluates to 1.
- D is meant to describe the relative natural frequency of positive examples of whatever we're trying to learn.

```
    t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
    Vectors assign variables to one of {0,1,*}.
    Concept $\mathcal{F}$ maps vectors to {0,1}.
```

- \* Assume  $\mathcal{D}$ , a probability distribution over all vectors  $\mathbf{v}$  which  $\mathcal{F}$  evaluates to 1.
- \* D is meant to describe the relative natural frequency of positive examples of whatever we're trying to learn.
- \* If we have a vector  $\mathbf{v}$  that describes a mallard, then  $\mathcal{D}(\mathbf{v}) = \text{relative frequency of mallards in the duck population.}$

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- + Concept  $\mathcal{F}$  maps vectors to  $\{0,1\}$ .
  - \* Assume  $\mathcal{D}$ , a probability distribution over all vectors  $\mathbf{v}$  which  $\mathcal{F}$  evaluates to 1.
  - \* D is meant to describe the relative natural frequency of positive examples of whatever \* Probability distribution D over all true vectors v.
  - \* If we have a vector  $\mathbf{v}$  that describes a mallard, then  $\mathcal{D}(\mathbf{v}) = \text{relative frequency of mallards in the universe.}$

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution  $\mathcal{D}$  over all true  $\mathbf{v}$ .

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution  $\mathcal{D}$  over all true  $\mathbf{v}$ .

# High-level Definitions.

## High-level Definitions.

+ A learning machine has two components:

## High-level Definitions.

- A learning machine has two components:
  - A learning protocol, or the method by which information is gathered from the world.

# High-level Definitions.

- A learning machine has two components:
  - A learning protocol, or the method by which information is gathered from the world.
  - A deduction procedure, or the mechanism for learning new concepts from gathered information.

# VALIANT'S LEARNING PROTOCOL

- t boolean variables p<sub>1</sub>,...,p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution  $\mathcal{D}$  over all true  $\mathbf{v}$ .

# VALIANT'S LEARNING PROTOCOL

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution  $\mathcal{D}$  over all true  $\mathbf{v}$ .

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution  $\mathcal{D}$  over all true  $\mathbf{v}$ .
  - Learner has access to two routines (or teachers):

- t boolean variables p<sub>1</sub>,...,p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution *D* over all true v.
  - Learner has access to two routines (or teachers):
  - 1.EXAMPLE: takes no input, returns a vector  $\mathbf{v}$  such that  $\mathcal{F}(\mathbf{v}) = \mathbf{1}$ .
    - \* Probability that EXAMPLE returns any particular v is  $\mathcal{D}(v)$ .

- t boolean variables p<sub>1</sub>,..., p<sub>t</sub>:
- Vectors assign variables to one of {0,1,\*}.
- Concept  $\mathcal{F}$  mapping vectors to  $\{0,1\}$ .
- Probability distribution *D* over all true v.
  - Learner has access to two routines (or teachers):
  - 1.**EXAMPLE**: takes no input, returns a vector  $\mathbf{v}$  such that  $\mathcal{F}(\mathbf{v}) = 1$ .
    - \* Probability that EXAMPLE returns any particular v is  $\mathcal{D}(v)$ .
  - 2.ORACLE: takes as input a vector  $\mathbf{v}$ , returns  $\mathcal{F}(\mathbf{v})$ .

$$\mathcal{F}(v) = is_a duck(v)$$

$$\mathcal{F}(v) = is_a_duck(v)$$

$$\mathcal{F}(v) = is_a duck(v)$$



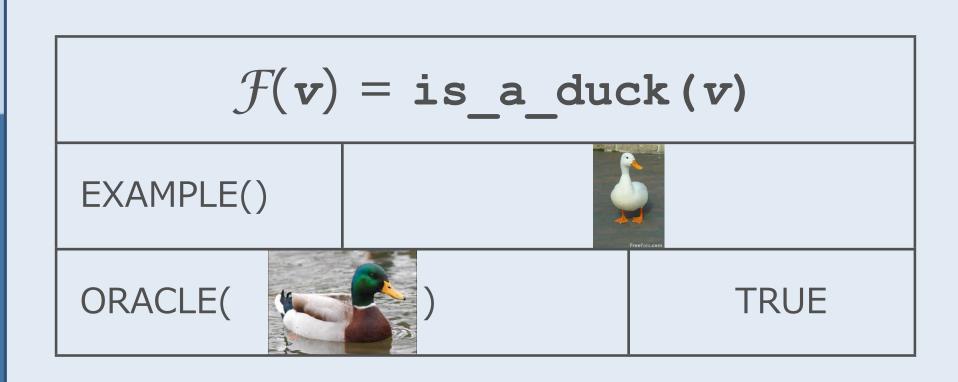
$$\mathcal{F}(\mathbf{v}) = is_a duck(\mathbf{v})$$

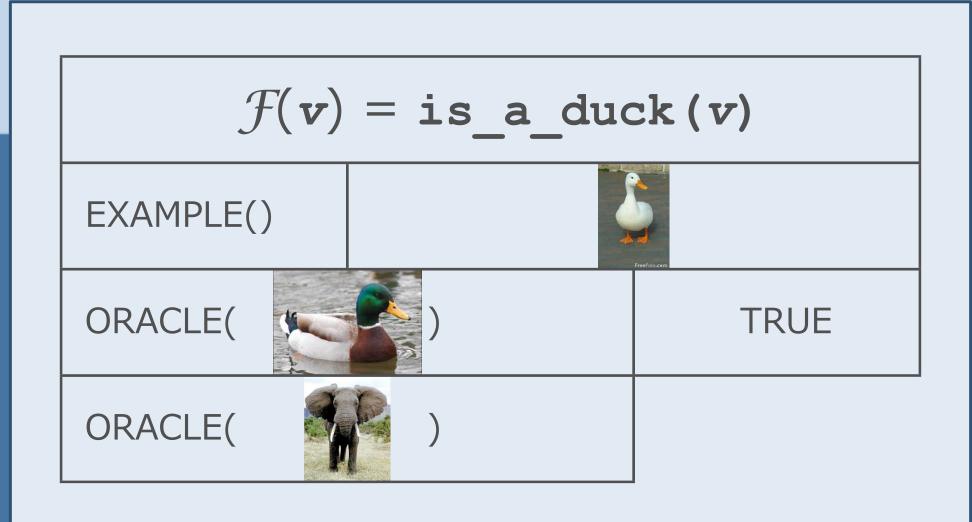
EXAMPLE()

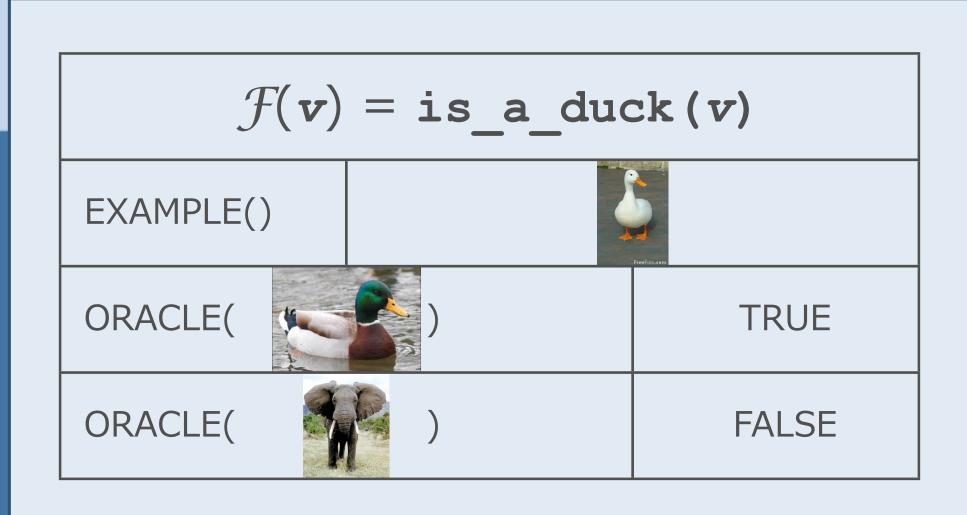


ORACLE(









$$\mathcal{F}$$
 = (a1 V a2)  $\wedge$  (a4 V a1)

$$\mathcal{F} = (a1 \lor a2) \land (a4 \lor a1)$$

$$\mathcal{F} = (a1 \lor a2) \land (a4 \lor a1)$$

$$\mathcal{F}$$
 = (a1 V a2)  $\wedge$  (a4 V a1)

EXAMPLE()

{a1=1, a2=0, a3=\*}

$\mathcal{F}$ = (a1 V a2) $\wedge$ (a4 V a1)			
EXAMPLE()	{a1=1, a2=0, a3=*}		
EXAMPLE()	{a1=0, a2=1, a3=*, a4=1}		

$$\mathcal{F} = (a1 \lor a2) \land (a4 \lor a1)$$

EXAMPLE()

{a1=1, a2=0, a3=\*}

EXAMPLE()

{a1=0, a2=1, a3=\*, a4=1}

ORACLE({a1=0,a2=0,a3=\*,a4=1})

$\mathcal{F}$ = (a1 V a2) $\wedge$ (a4 V a1)			
EXAMPLE()	{a1=1, a2=0, a3=*}		
EXAMPLE()	{a1=0, a2=1, a3=*, a4=1}		
ORACLE({a1=0,a2=0,a3=*,a4=1})		FALSE	

A class of problems is Probably Approximately
 Learnable if instances of the problem can be learned by a deduction algorithm that:

- A class of problems is Probably Approximately
   Learnable if instances of the problem can be learned by a deduction algorithm that:
  - Uses this protocol.

- A class of problems is Probably Approximately
   Learnable if instances of the problem can be learned by a deduction algorithm that:
  - Uses this protocol.
  - Runs in reasonable time: polynomial by adjustable parameter h, size of learned program, and number of variables determined in the learned formula.

- A class of problems is Probably Approximately
   Learnable if instances of the problem can be learned by a deduction algorithm that:
  - Uses this protocol.
  - Runs in reasonable time: polynomial by adjustable parameter h, size of learned program, and number of variables determined in the learned formula.
  - Produces a program that says something is false when it's true with probability no greater than (1-h-1); never says that something is true when it's false.

We are trying to make a program (learning machine)
that can learn, in polynomial time, another program
(the learned program) that recognizes whether a
boolean formula (concept) is true for any set of
boolean data.

- We are trying to make a program (learning machine)
  that can learn, in polynomial time, another program
  (the learned program) that recognizes whether a
  boolean formula (concept) is true for any set of
  boolean data.
- The learning program has access to a function that will give it a bunch of examples, as well as a function that will check its work.

- We are trying to make a program (learning machine)
  that can learn, in polynomial time, another program
  (the learned program) that recognizes whether a
  boolean formula (concept) is true for any set of
  boolean data.
- The learning program has access to a function that will give it a bunch of examples, as well as a function that will check its work.
- \* The learning machine can learn a program that is sometimes wrong, so long as the probability that the learned program is ever wrong is adjustable.

- 1. General framework for defining Learning Machines, or programs that can learn/write/produce other programs of a particular type.
  - A Learning Machine for animal recognition, for example, might learn to write a program that recognizes whether a given animal is a duck.
- 2. Definition of a particular learning protocol.
- 3. Definition of when a program class is reasonably-learnable.
- 4. Definition/proofs of reasonably-learnable program classes.

- 1. General framework for defining Learning Machines, or programs that can learn/write/produce other programs of a particular type.
  - A Learning Machine for animal recognition, for example, might learn to write a program that recognizes whether a given animal is a duck.
- 2. Definition of a particular learning protocol.
- 3. Definition of when a program class is reasonably-learnable.
- 4. Definition/proofs of reasonably-learnable program classes.

1. General framework for defining Learning Machines, The paper proves three different program classes probably-approximately-learnable.

- 1. General framework for defining Learning Machines,
  - The paper proves three different program classes probably-approximately-learnable.
  - \* I am not going to walk through the proofs; they are by construction of deduction algorithms that can learn the given programs and proofs of their bounds.
- 2
- 3.
- 4.

#### Outline

- 1. General framework for defining Learning Machines,
  - + The paper proves three different program classes probably-approximately-learnable.
  - \* I am not going to walk through the proofs; they are by construction of deduction algorithms that can learn the given programs and proofs of their bounds.
- \* I am going to give the upper bounds of the algorithms. This requires a definition of a function.
- 4.

#### Outline

- 1. General framework for defining Learning Machines,
  - + The paper proves three different program classes probably-approximately-learnable.
  - \* I am not going to walk through the proofs; they are by construction of deduction algorithms that can learn the given programs and proofs of their bounds.
- I am going to give the upper bounds of the algorithms. This requires a definition of a function.
  - The proof of that function's upper bound is the major lemma in all three proofs, so I will outline it.
- 4.

#### Outline

- 1. General framework for defining Learning Machines,
  - + The paper proves three different program classes probably-approximately-learnable.
  - \* I am not going to walk through the proofs; they are by construction of deduction algorithms that can learn the given programs and proofs of their bounds.
- 2. I am going to give the upper bounds of the algorithms. This requires a definition of a function.
  - The proof of that function's upper bound is the major lemma in all three proofs, so I will outline it.
- 4. This means the next 3 slides are mathy.

### A Combinatorial Bound

#### A Combinatorial Bound

L(h,s) is a function defined for all real numbers h >
 1 and integers s > 1.

#### A Combinatorial Bound

- L(h,s) is a function defined for all real numbers h >
   1 and integers s > 1.
- + Returns smallest integer n such that in n independent Bernoulli trials, each with probability at least  $h^{-1}$  of success, P(< s successes)  $< h^{-1}$ 
  - Bernoulli trial: an experiment whose outcomes are either "success" or "failure"; randomly distributed by some probability function.

$$L(h,S) \leq 2h(S + \log_e h)$$

$$L(h,S) \leq 2h(S + \log_e h)$$

Proof by algebraic substitution of well-known inequalities:

$$L(h,S) \leq 2h(S + \log_e h)$$

Proof by algebraic substitution of well-known inequalities:

$$1. \forall x > 0, (1 + x^{-1})^x < e$$

$$L(h,S) \leq 2h(S + \log_e h)$$

Proof by algebraic substitution of well-known inequalities:

$$1. \forall x > 0, (1 + x^{-1})^x < e$$

$$2. \forall x > 0, (1 - x^{-1})^{x} < e^{-1}$$

$$L(h,S) \leq 2h(S + \log_e h)$$

Proof by algebraic substitution of well-known inequalities:

$$1. \forall x > 0, (1 + x^{-1})^x < e$$

$$2. \forall x > 0, (1 - x^{-1})^x < e^{-1}$$

3. In m independent trials, each with success probability  $\geq p$ :

$$\mathbf{P}(\text{successes at most } \mathbf{k}) \leq \left(\frac{\mathbf{m} - \mathbf{mp}}{\mathbf{m} - \mathbf{k}}\right)^{\mathbf{m} - \mathbf{k}} \left(\frac{\mathbf{mp}}{\mathbf{k}}\right)^{\mathbf{k}}$$

+ L(h, s) is basically linear in both h and s.

- + L(h, S) is basically linear in both h and S.
- Applies to using EXAMPLEs and ORACLE to determine vectors.

- + L(h, S) is basically linear in both h and S.
- Applies to using EXAMPLEs and ORACLE to determine vectors.
- \* An algorithm can approximate the set of determined variables in natural EXAMPLEs of  $\mathcal{F}$  in runtime independent of *total* number of variables in the world.

- + L(h, S) is basically linear in both h and S.
- Applies to using EXAMPLEs and ORACLE to determine vectors.
- \* An algorithm can approximate the set of determined variables in natural EXAMPLEs of  $\mathcal{F}$  in runtime independent of *total* number of variables in the world.
  - Dependent only the number of variables that are determined in  $\mathcal{F}$ .

## Remaining Question

Given that learning protocol, what classes of tasks are learnable in polynomial time?

1. *k*-CNF expressions

- 1. k-CNF expressions
- 2. Monotone DNF expressions

- 1. *k*-CNF expressions
- 2. Monotone DNF expressions
- 3. µ-expressions

# *k*–CNF Expressions

# *k*-CNF Expressions

Conjunctive Normal form (CNF):

$$(a_1 \ \lor \ a_2 \ \lor \ a_3) \ \land \ (a_4 \ \lor \ a_1) \ ...$$

## k-CNF Expressions

Conjunctive Normal form (CNF):

$$(a_1 \lor a_2 \lor a_3) \land (a_4 \lor a_1) ...$$

 \* k-CNF expression: a CNF expression where each internal clause is composed of ≤ k literals.

## k-CNF Expressions

Conjunctive Normal form (CNF):

```
(a_1 \lor a_2 \lor a_3) \land (a_4 \lor a_1) \dots
```

- \* k-CNF expression: a CNF expression where each internal clause is composed of ≤ k literals.
- \* Learnable with an algorithm that does not call ORACLE, and calls EXAMPLE  $\leq L(h, 2t^{k+1})$  times. (t is the number of variables)

Disjunctive Normal Form (DNF):

$$(a_1 \wedge a_2 \wedge a_3) \vee (a_1 \wedge a_4) \dots$$

Disjunctive Normal Form (DNF):

$$(a_1 \wedge a_2 \wedge a_3) \vee (a_1 \wedge a_4) \dots$$

 An expression is monotone if it contains no negated literals.

Disjunctive Normal Form (DNF):

```
(a_1 \wedge a_2 \wedge a_3) \vee (a_1 \wedge a_4) \dots
```

- An expression is monotone if it contains no negated literals.
- Learnable with an algorithm that calls
   EXAMPLES L = L(h,d) times and ORACLES
   d\*t times, where d is the degree of the
   expression and t is the number of variables.

+ General expression over  $\{p_1, ..., p_t\}$  defined recursively  $(1 \le i \le t)$ :

```
f := p_i \mid \sim p_i \mid f_1 \land f_2 \mid f_1 \lor f_2
```

General expression over {p<sub>1</sub>,...,p<sub>t</sub>} defined recursively (1 ≤ i ≤ t):

$$f := p_i \mid \sim p_i \mid f_1 \land f_2 \mid f_1 \lor f_2$$

A μ-expression is an expression in which each
 p appears at most once.

General expression over {p<sub>1</sub>,...,p<sub>t</sub>} defined recursively (1 ≤ i ≤ t):

```
f := p_i \mid \sim p_i \mid f_1 \land f_2 \mid f_1 \lor f_2
```

- A μ-expression is an expression in which each
   p appears at most once.
- Learnable with an exactly correct algorithm that calls two slightly more powerful ORACLE functions O(t³) times total.

 Learnability theory is concerned with what programs can be learned automatically.

- Learnability theory is concerned with what programs can be learned automatically.
- We should reason about what is programmatically learnable in the same way we reason about what is computable.

- Learnability theory is concerned with what programs can be learned automatically.
- We should reason about what is programmatically learnable in the same way we reason about what is computable.
- A class of programs is Probably Approximately Learnable when, using a particular type of teacher, a given algorithm can learn a program that can recognize instances of that class with a certain probability.

- Learnability theory is concerned with what programs can be learned automatically.
- We should reason about what is programmatically learnable in the same way we reason about what is computable.
- \* A class of programs is Probably Approximately Learnable when, using a particular type of teacher, a given algorithm can learn a program that can recognize instances of that class with a certain probability.
- 3 examples of such learnable program types are k-CNF expressions, monotone DNF expressions, and μexpressions.

#### Interesting Concluding Questions

- What else is learnable by these definitions?
- Is the definition of "learnable" reasonable?
  - How powerful should the teachers be?
  - What about if we use negative in addition to positive examples?
- + How do humans learn?

\* Assume we have urn that contains many marbles of s different types. We want to "learn" the different types of marbles by taking a small random sample x, of size sufficient that, with high probability, it contains at least 99% of s marble type representatives.

- \* Assume we have urn that contains many marbles of s different types. We want to "learn" the different types of marbles by taking a small random sample x, of size sufficient that, with high probability, it contains at least 99% of s marble type representatives.
- Definition of L(h, S) implies:

```
|X| = L(100,S) \Rightarrow P(succeeded overall) > 99%
```

- \* Assume we have urn that contains many marbles of s different types. We want to "learn" the different types of marbles by taking a small random sample x, of size sufficient that, with high probability, it contains at least 99% of s marble type representatives.
- Definition of L(h, S) implies:

```
|X| = L(100,S) \Rightarrow P(succeeded overall) > 99%
```

\* "Success" for each trial is defined as picking a marble we haven't picked before. Success clearly depends on previous choices, but the probability of each success will always be at least 1%, independent of previous choices.