CS 710: Complexity Theory 2/4/2010

Lecture 6: Alternation

Instructor: Dieter van Melkebeek Scribe: Ashutosh Kumar

The last few lectures were devoted to the study of the non deterministic models of computations (NTM) and the associated complexity classes. In this lecture, we generalize this model/associated classes of langauges to capture the notion of alternation. We start by extending the class NP to a more general class: Polynomial hierarchy (PH). After establishing a few simple results about this hierarchy, we describe a model of computation, called alternating Turing machines (ATM), which captures the class PH in the same way as non-deterministic Turing machines capture the class NP. We derive a few basic results for the classes of problems that can be solved using alternation. We discuss a few other characterizations of the polynomial hierarchy and describe a complete problem at each level of PH. Finally, we sketch a few results that relate the complexity classes associated with the alternating model to some previously defined complexity classes.

1 Motivation

We have already seen that the class NP can be identified with the class of those languages which have polynomial time verifiers. For example, although, testing a boolean expression $\phi = \phi(p_1, ..., p_n)$ for satisfiability (SAT) is (seemingly) hard, checking if ϕ evaluates to true under a given valuation, is easy. Moreover, to check if ϕ is satisfiable, the number of valuations that need to be fed to the verifier is $\mathcal{O}(2^{|\phi|})$. More generally, we had the following result:

A language $L \in$ NP iff there exists a constant $c > 0$ and a polynomial time verifier $V \in$ P such that $x \in L \Leftrightarrow (\exists y \in \Sigma^{\leq |x|^c})\langle x, y\rangle \in V$.

As an example of a problem which doesn't appear to be in NP (though this is open), consider the problem of boolean formula minimization - denoted by MIN-FORM:

$$\phi \in \text{MIN-FORM} \Leftrightarrow \forall \psi(|\psi| < |\phi| \rightarrow \exists x(\phi(x) \neq \psi(x))) \tag{1}$$

The length of any formula ψ that is smaller than ϕ is at most $|\phi|$. The length of a valuation x for ϕ is also bounded by $|\phi|$. Moreover, checking for a given pair (ψ, x) whether $\phi(x) = \psi(x)$ can be done in polynomial time (It takes two SAT verifications followed by a test of equality). So one has the following:

$$\phi \in \text{MIN-FORM} \Leftrightarrow (\forall y \in \Sigma^{\leq |\phi|^c})(\exists x \in \Sigma^{\leq |\phi|^c})\langle \phi, y, x\rangle \in V \text{ for some } V \in \text{P} \tag{2}$$

If we compare the quantifier complexity of the above formula describing the membership relation in MIN-FORM, with the ones that represent languages in NP, we notice that the former (MIN-FORM) has an extra universal quantifier - more importantly, there is a quantifier alternation. The class NP can be thought of as the result of closing the class of predicates in P under poly-bounded projections (arising from the existential quantifier). One may, in a similar way, consider languages that result from applying a poly-bounded universal quantifier to predicates in NP and so on. This results in the polynomial hierarchy which will be described below. It is important to note that it's the number of quantifier alternations followed by a predicate in P that really matters here since a chain of existential (resp. universal) quantifiers can be replaced by one existential (resp. universal) quantifier with a trivial reduction in the arity of the quantifier free predicate.

2 The Polynomial Hierarchy

We define a hierarchy of general complexity classes $\{Q_k^p | k \geq 0\}$. The class Q_k^p is defined as the set of those languages whose membership constraints can be expressed by using formulas with $k \geq 0$ alternate existential and universal quantifiers, with each quantified variable of size polynomial in the length of the input, and the initial quantifier being existential for $Q = \Sigma$ and universal for $Q = \Pi$.

A more precise description of Σ_k^p and Π_k^p follows:

Definition 1. *We say that a language L is in Σ_k^p if for every $x \in \Sigma^*$*

$$x \in L \Leftrightarrow (\exists y_1 \in \Sigma^{\leq |x|^c})(\forall y_2 \in \Sigma^{\leq |x|^c}) \ldots (Q y_k \in \Sigma^{\leq |x|^c})(\langle x, y_1, y_2, \ldots y_k \rangle \in V)$$

for some $V \in \mathrm{P}$ and some constant c.

Definition 2. *We say that a language L is in Π_k^p if for every $x \in \Sigma^*$*

$$x \in L \Leftrightarrow (\forall y_1 \in \Sigma^{\leq |x|^c})(\exists y_2 \in \Sigma^{\leq |x|^c}) \ldots (Q y_k \in \Sigma^{\leq |x|^c})(\langle x, y_1, y_2, \ldots y_k \rangle \in V)$$

for some $V \in \mathrm{P}$ and some constant c.

Notes: The quantifier Q for y_k in Σ_k^p is $\exists$ if k is odd and $\forall$ if k is even. A dual statement holds for Π_k^p. The super-script p in Σ_k^p and Π_k^p denotes the class P. There is a small notational inconsistency. Σ is used to denote a class of problems as well as to denote the input alphabet. But the intended usage is usually clear from context.

If $k = 0$, there are no quantified variables and the verifier V can decide membership just by looking at the input. In other words, V is an algorithm for L and Σ_0^p is the same as P. In the absence of any quantifiers, there is no real distinction between existential and universal quantification. Thus, $\Sigma_0^p = \Pi_0^p = \mathrm{P}$.

The definition of Σ_1^p is exactly the same as that of NP given earlier and so, $\Sigma_1^p = \mathrm{NP}$. We will shortly see that $\Pi_1^p = \mathrm{coNP}$. It is also clear that MIN-FORM $\in \Pi_2^p$. The following proposition shows that Q_k^p form a hierarchy.

Proposition 1. $\Pi_k^p \subseteq \Pi_{k+1}^p$ *and* $\Sigma_k^p \subseteq \Sigma_{k+1}^p$

This is trivial since one may, for example, add an appropriate quantifier with respect to a new variable y_{k+1} in front of the predicate V which will be ignored by V. Since the basic classes $\Sigma_0^p = \Pi_0^p = \mathrm{P}$ are closed under complementation one gets the following:

Proposition 2. $\Sigma_k^p = co\Pi_k^p$ *and* $\Pi_k^p = co\Sigma_k^p$

Notice that the complement of a language in Q_k^p corresponds to the negation of the Q_k^p predicate that represents it. This amounts to flipping the quantifiers and replacing the predicate V by its negation.

Proposition 3. $\Sigma_k^p \cup \Pi_k^p \subseteq \Sigma_{k+1}^p \cap \Pi_{k+1}^p$

We can transform the membership constraint for Σ_k^p to that of: (1) Σ_{k+1}^p by adding a universally quantified variable that is not used by V in the end; (2) Π_{k+1}^p by adding a universally quantified variable that is not used by V in the beginning. Hence $\Sigma_k^p \subseteq \Sigma_{k+1}^p \cap \Pi_{k+1}^p$. A similar argument applies for Π_k^p and hence the above result holds.

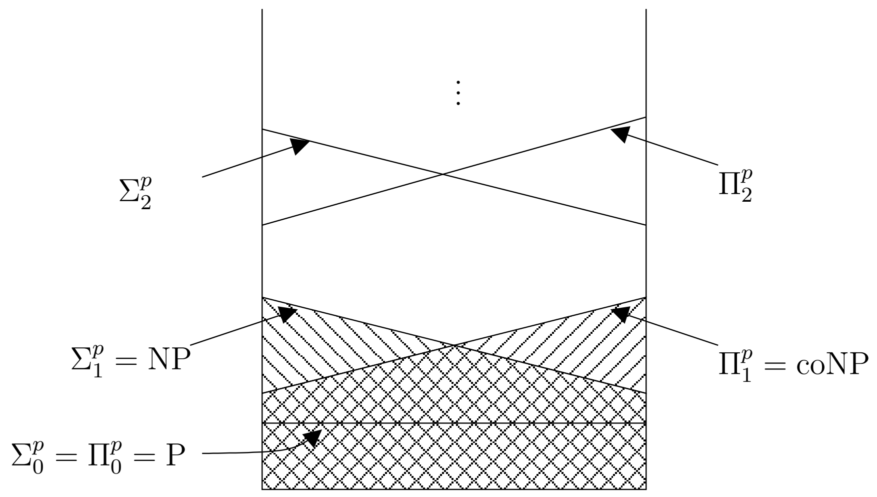
$\vdots$
Σ_2^p
Π_2^p
$\Sigma_1^p = \mathrm{NP}$
$\Pi_1^p = \mathrm{coNP}$
$\Sigma_0^p = \Pi_0^p = \mathrm{P}$

Figure 1: Pictorial illustration of the polynomial hierarchy

Propositions 1 and 3 can be illustrated using Figure 1. The k^{th} line sloping upwards bounds languages in Π_k^p and the k^{th} line sloping downwards bounds Σ_k^p. Both these lines are above the lines at the previous levels. For $k = 0$, the two lines collapse into each other, as $\mathrm{P} = co\mathrm{P}$.

Corollary 1. $\Pi_1^p = \mathrm{coNP}$*, since we already derived that* $\Sigma_1^p = \mathrm{NP}$

One may ask if the inclusion in Proposition 1 is strict, i.e. whether $\Sigma_k^p \subset \Sigma_{k+1}^p$. Even the simplest version of this question, for $k = 1$ ($\mathrm{P} \neq \mathrm{NP}$) is open, as mentioned in previous lectures. The class PH is defined to be the union of $\{\Sigma_k^p | k \geq 0\}$ (equivalently $\{\Pi_k^p | k \geq 0\}$):

Definition 3. PH *is the class of all problems in the* polynomial hierarchy *: any fixed number of alternations are allowed. i.e.* $\mathrm{PH} = \bigcup_k \Sigma_k^p$

Note: We need not include Π_k^p in the previous definition as a consequence of Proposition 2

Theorem 1. *If* $\Sigma_k^p = \Pi_k^p$ *for some* $k \geq 1$ *then* $\mathrm{PH} = \Sigma_k^p$*, in other words, the polynomial time hierarchy collapses to level* k*.*

Proof. It suffices to show that for every $k \geq 1$ if $\Sigma_k^p = \Pi_k^p$ then $\Sigma_k^p = \Sigma_{k+1}^p = \Pi_{k+1}^p$. So fix an arbitrary $k \geq 1$ and consider a language $L \in \Sigma_{k+1}^p$. A string $x \in L$ iff for some constant c and $V \in P$ the following holds:

$$(\exists y_1 \in \Sigma^{\leq |x|^c})(\forall y_2 \in \Sigma^{\leq |x|^c}) \ldots (Q y_k \in \Sigma^{\leq |x|^c})(\overline{Q} y_{k+1} \in \Sigma^{\leq |x|^c})(\langle x, y_1, y_2, \ldots y_k, y_{k+1}\rangle \in V) \quad (3)$$

Notice that $(\forall y_2 \in \Sigma^{\leq |x|^c}) \ldots (Q y_k \in \Sigma^{\leq |x|^c})(\overline{Q} y_{k+1} \in \Sigma^{\leq |x|^c})(\langle x, y_1, y_2, \ldots y_k, y_{k+1}\rangle \in V)$ is a Π_k predicate on input $\langle x, y_1\rangle$. Because $\Sigma_k^p = \Pi_k^p$, there is an equivalent Σ_k^p predicate ϕ on input

$\langle x, y_1 \rangle$. The existential quantification in equation 3 (there's one since $k \geq 1$) can be merged with the initial existential quantifier of ϕ, thus leaving a new Σ_k^p predicate ϕ' on input $\langle x \rangle$. It follows that if $\Sigma_k^p = \Pi_k^p$, then every Σ_{k+1}^p language can be expressed using a Σ_k^p predicate. Thus, $\Sigma_{k+1}^p \subseteq \Sigma_k^p$. Combining this with proposition 1, we get $\Sigma_k^p = \Sigma_{k+1}^p$. ☐

Corollary 2. *If* $\mathrm{P} = \mathrm{NP}$ *then* $\mathrm{PH} = \mathrm{P}$.

Proof. Suppose P = NP. Then NP = coNP. It follows from the above theorem that PH collapses to NP and therefore, to P. ☐

From the above corollary, we conclude that if PH does not collapse then $\mathrm{P} \neq \mathrm{NP}$. But the former seems to be a stronger statement. That is, even if $\mathrm{P} \neq \mathrm{NP}$, the polynomial hierarchy may collapse to some other class. But the general conjecture in the community is that PH does not collapse. In fact there have been results that start from some assumption and derive that PH collapses in order to disprove the likeliness of that assumption.

3 Completeness

We provide an example of a problem that is complete in Σ_k^p.

Definition 4. *$T.\Sigma_k$ is the set of all true, fully quantified Σ_k boolean formulas - i.e. Σ_k boolean sentences, where the quantifier free boolean predicate could be taken to be a (1) CNF if k is odd and (2) DNF if k is even - This doesn't make any difference.*

Similarly, we can define $T.\Pi_k$ as the set of all true Π_k boolean sentences.

Claim 1. *$T.\Sigma_k$ is $\leq_m^p$-complete for Σ_k^p and $T.\Pi_k$ is $\leq_m^p$-complete for Π_k^p.*

Proof. Consider a language $L \in \Sigma_k^p$ with associated verifier V. Suppose k is odd. Then the last quantifier is $\exists$, and the last quantifier together with V is $(\exists y_k \in \Sigma^{\leq |x|^c})(\langle x, y_1, y_2, ..., y_k \rangle \in V)$. This is an NP statement, so by the NP-completeness of SAT can be converted in polynomial time into the statement $(\exists z \in \{0,1\}^{\leq |x|^d})\phi_x(\langle \overline{y_1}, \overline{y_2}, ..., \overline{y_{k-1}}, \overline{z} \rangle)$ where ϕ_x is a boolean formula (depending on x) and d is some constant. Then $(\exists \overline{y_1} \in \{0,1\}^{\leq |x|_1^c})(\forall \overline{y_2} \in \{0,1\}^{\leq |x|_2^c})...(\exists \overline{z} \in \{0,1\}^{\leq |x|^d})\phi_x(\langle \overline{y_1}, \overline{y_2}, ..., \overline{y_{k-1}}, \overline{z} \rangle)$ is a a $T.\Sigma_k$ instance that is true if and only if $x \in L$.

The case when k is even is dealt with in a similar fashion by using the coNP completeness of TAUTOLOGY.

As this reduction can be accomplished in polynomial time, $T.\Sigma_k$ is hard for Σ_k^p under $\leq_m^p$. It's obviously in Σ_k^p since the truth value of a quantifier free boolean predicate can be checked in polynomial time. ☐

4 Alternate Characterizations

4.1 Using Oracle Machines

Claim 2. $\Sigma_{k+1}^p = \mathrm{NP}^{\Sigma_k^p}$. *In other words, the set of languages in the $(k+1)^{th}$ level of the polynomial hierarchy is the set of languages recognized by non-deterministic machines with access to oracles at the k^{th} level.*

Proof. For $k = 0$, the statement is $\mathrm{NP} = \mathrm{NP}^{\mathrm{P}}$. $\mathrm{NP} \subseteq \mathrm{NP}^{\mathrm{P}}$ is trivial because we can simply choose to ignore the oracle. $\mathrm{NP}^{\mathrm{P}} \subseteq \mathrm{NP}$ because the time complexity of the oracle will, in worst case, increase the degree of the polynomial in the time complexity.

The statement is non-trivial for $k > 0$. Consider $k = 1$. Suppose we have a language $L \in \Sigma_2^p$. Then, for some $c > 0$ and $V \in \mathrm{P}$,

$$x \in L \Leftrightarrow (\exists y_1 \in \Sigma^{\leq |x|^c})(\forall y_2 \in \Sigma^{\leq |x|^c})(\langle x, y_1, y_2 \rangle \in V)$$

We can construct a non-deterministic TM M that guesses the value of y_1 and tries to solve $(\forall y_2 \in \Sigma^{\leq |x|^c})\langle x, y_1, y_2 \rangle \in V$. The latter is a Π_1 formula and can be solved using an oracle for Σ_1^p because $\Sigma_1^p = co(\Pi_1^p)$ and in general any language can be solved given an oracle to its complement. Thus, $L \in \mathrm{NP}^{\Sigma_1^p}$.

Suppose $L \in \mathrm{NP}^{\Sigma_1^p}$. We can express that L is decidable in Σ_2^p as follows:

1. Express the computation path followed by the base NP machine as a Σ_1 formula by guessing the queries made by the machine, as well as the results of the queries.

2. Express the constraints that positive query responses are valid, again by using a Σ_1 predicate.

3. Express the constraints that negative query responses are valid by using a Π_1 predicate. The universal quantifier is required because in this step, we want to ensure the non-existence of a witness to the query, rather than its existence.

Overall a Σ_2 predicate expresses the decidability of L, and $L \in \Sigma_2^p$. Thus, $\Sigma_2^p = \mathrm{NP}^{\Sigma_1^p}$. (The right hand side can also be written as $\mathrm{NP}^{\mathrm{NP}}$).

Arguments for $k \geq 2$ are similar. ☐

4.2 Using Boolean Circuits

Claim 3. *Any language $L \in \Sigma_k^p$ can be expressed as an exponential size boolean circuit, with $k+1$ alternating levels of AND and OR gates of unbounded fan-in, with the last level having polynomial bounded fan-in and such that each bit of the circuit description can be computed in polynomial time, and vice-versa.*

Proof. Consider a language $L \in \Sigma_k^p$ with verifier V. We can construct an enormous boolean circuit as follows: an exponential number of polynomial circuits evaluating membership in V for all possible combinations of $y_1, y_2, \ldots y_k$ and a specific value for x. We can make these polynomial circuits to have only two levels by expressing the function $V(x, y_1, y_2, \ldots y_k)$ in CNF or DNF. The outputs of these circuits are combined hierarchically at k levels to leave a single output at the top-most level. This output is the decision whether $x \in L$. The i^{th} level contains an array of AND gates if y_i is universally quantified and an array of OR gates if y_i is existentially quantified. The number of gates in the i^{th} level is equal to the number of choices for inputs $y_1, y_2, \ldots y_{i-1}$. By appropriately choosing a CNF or DNF for the verifier V, we can merge the gates from the k^{th} level with the top gates from the normal form that is chosen. It can be verified that each bit is poly-time computable.

Now, consider a boolean circuit as described above with an OR gate at the top-most level. We must construct a Σ_k formula to compute the language decided by the circuit, i.e. we need to determine how many bits to guess for the $\exists$ and $\forall$ quantifiers and what the V will be. Consider the top-most OR gate. Its output will be 1 if there exists a gate at the lower level whose output is 1. We can express this as

$$(\exists G_2)(\text{output of gate } G_2 \text{ is } 1) \tag{4}$$

where G_2 is a second level gate. G_2 will be an AND gate. It will produce an output 1 if all the OR gates at the third level produce an output 1. So, stmt. 4 becomes:

$$(\exists G_2)(\forall G_3)(\text{output of gate } G_3 \text{ is } 1) \tag{5}$$

where G_3 is any gate whose output is connected as input to the chosen G_2. Since the circuit is of exponential circuit, we can represent gates in the circuit using polynomial size indices. If we repeatedly apply these steps, we will get a Σ_k predicate with the final verification task being that of evaluating the output of the gate at the $(k+1)^{th}$ level. Since each bit of the circuit description is computable in polynomial time, we can use the choices of the indices at each level to identify the gate that needs to be evaluated as well as the bits from the input that go into that gate. Thus, we can evaluate the last predicate of the Σ_k formula in poly-time. Thus, we have a Σ_k^p language corresponding to the circuit. Similarly we can construct a Π_k^p language corresponding to a circuit with an AND gate at the top-most level. □

4.3 Alternating Turing Machines

In this section, we extend the class of non-deterministic Turing machines (NTM) to model alternation. This model of computation will also capture the polynomial hierarchy under polynomial time constraint. An alternating TM (ATM) can be thought of as an NTM with an extra attribute: every non-halting state is described as being an existential state or a universal state but not both. The transition function of this machine has the same definition as that of an NTM. A configuration of the machine is accepting if either:

1. This is a halting configuration and the machine is in an accepting state, or
2. The current state is existential and at least one computation path from this state leads to an accepting configuration, or
3. The current state is universal and all computation paths from this state lead to an accepting configuration.

The machine itself accepts an input if the initial configuration is accepting. The following gives our final characterization of Σ_k^p and Π_k^p.

Claim 4. $\Sigma_k^p = \{L | L$ *is accepted by an alternating TM with an existential start state that runs in polynomial time and has at most* $k-1$ *quantifier alternations*$\}$
$\Pi_k^p = \{L | L$ *is accepted by an alternating TM with a universal start state that runs in polynomial time and has at most* $k-1$ *quantifier alternations*$\}$

Proof. Consider a language $L \in \Sigma_k^p$. We can construct a k stage alternating TM M with the i^{th} stage guessing the value of y_i. To match the quantifier of the y_i's, all the states in the i^{th} stage must be existential if i is odd and universal if i is even. The verifier V of L does not require any non-determinism. So, the states that simulate V can be made existential or universal depending on k. Thus, M recognizes L and has an existential start state and performs at most $k-1$ alternations.

Similarly, we can construct an alternating TM that recognizes a language in Π_k^p and satisfies the above constraints.

Consider an alternating TM M that performs at most $k-1$ alternations. We can construct an equivalent Σ_k^p or Π_k^p language L as follows. If M halts in polynomial time, the time it spends in each stage of the alternation is also polynomial. We can model the choices made by M in the i^{th} step as a polynomial length string y_i. If i^{th} step is existential (resp. universal), then y_i is quantified existentially (resp. universally). The verifier V has to verify that the choices made are valid for the given input and machine M and also that the final state is halting and accepting. This can be done in polynomial time. The resulting formula is a Σ_k formula if M's initial state is existential, and is a Π_k formula otherwise. □

5 Time and Space

Using the same definition of time and space required by a Turing machine we can define complexity classes Σ_k-TIME(t) and Σ_k-SPACE(s). We can also derive hierarchy results using the same technique used earlier, namely delayed diagonalization. These results get simplified if we allow an unlimited number of alternations. We can define ATIME(t) as the set of problems that can be solved in time t on an alternating TM with any number of quantifier alternations. ASPACE(s) is the set of all problems that can be solved using space s on an alternating TM with any number of quantifier alternations.

Some results on Time and Space

Theorem 2. *NSPACE*$(s) \subseteq$ *ATIME*(s^2)

Proof. This follows from our proof of NSPACE$(s) \subseteq$ DSPACE(s^2) in last lecture. Recall that we constructed a formula very similar to a Σ_k formula in our divide-and-conquer formulation of that proof. The existential quantifier guessed an intermediate configuration ($\mathcal{O}(s)$ long) of the Turing machine and the universal quantifier was used to specify two independent reachability conditions (1 bit is enough). There were $\mathcal{O}(s)$ such quantifiers. The final predicate verifies whether the transition from one configuration to another is valid, which takes $\mathcal{O}(s)$ time since each configuration is $\mathcal{O}(s)$ long. Thus the guessing stages of the machine take $\mathcal{O}(s^2)$ time and the verification at the end takes $\mathcal{O}(s)$ time, for a total running time of $\mathcal{O}(s^2)$. □

Theorem 3. *ATIME*$(t) \subseteq$ *DSPACE*(t^2)

Proof. Let M be an alternating machine running in time t. If we separate M's execution into existential and universal stages, there are at most t many and each is at most t long. We begin by simulating M as long as it remains within the first stage. For the second stage of M, we simulate it for all possible choices from the first stage. There were at most t separate choices, so we can cycle through all of these using space $\mathcal{O}(t)$. For the third stage of M, we must simulate it for all possible choices in the first and second stages. It takes space $\mathcal{O}(t+t)$ to cycle through all of these. As there are a total of at most t stages, we can cycle through all possible guesses of M using $\mathcal{O}(t^2)$ space. For the guesses corresponding to an existential stage, we ensure that at least one of the guesses results in an accepting computation; for the guesses corresponding to a universal stage, we ensure that all of the guesses result in an accepting computation.

Given a sequence of guesses, we simulate M with these guesses using the space-efficient universal Turing Machine from the first lecture. If we first convert M into an equivalent machine M' that uses $O(t)$ space, the total space usage is $\mathcal{O}(t^2 + s_M) = \mathcal{O}(t^2 + t) = \mathcal{O}(t^2)$. $\square$

Corollary 3. *PSPACE = AP*

Proof. From Theorem 3, AP $\subseteq$ PSPACE. But since PSPACE $\subseteq$ NSPACE, from Theorem 2, we get PSPACE $\subseteq$ AP. $\square$

Theorem 4. $ASPACE(s(n)) = \bigcup_{c>0} \mathrm{DTIME}(2^{c.s(n)})$. *In other words, we need time exponential in the space requirement to deterministically simulate an alternating TM.*

Proving this theorem will be a homework problem.

Corollary 4. *AL = P*

Corollary 5. *APSPACE = EXP*

6 Next Lecture

Next time, we will use alternation to prove the non-existence of SAT-solvers that are both time and space efficient. The main topic of next class is non-uniformity where we allow different algorithms for inputs of different lengths.