S̃tudy Notes

Last updated on : April 17, 2014

1 English Vocabulary

This is study notes on The Structure of English Words (LING150) course from http://darkwing.uoregon.edu/ l150web/index.html

1.1 Course Organization

- **Unit 1:** Basic Word Analysis
  - Historical sources of English words
  - Basic principles of word analysis (morphology)
- **Unit 2:** Intermediate Word Analysis and Basic Phonetics
  - Alternations in morpheme forms (allomorphy)
  - Basic principles of English sounds (phonetics)
- **Unit 3:** Advanced Word Analysis and Semantic Change
  - More alternations in morpheme forms (allomorphy rules)
  - Historical changes of meanings (semantic change)
- **Unit 4:** - The Origins and History of English
  - Pre-history of English and Indo-European languages
  - English history

1.2 Introduction to English vocabulary

1.2.1 Sources of English words

- Native words
- Borrowed Words
  - Exotic Languages
  - Classic Languages
    - Greek
    - Latin

The native words are words which are used in evryday conversations. The native words falls into follwoing categories.

Type	**Example**
Body Parts	Foot, mouth, hand, leg
Family Relationships / Kinship terms	Father, mother, brother, sister
Everyday, Natural objects	rock, house, hill
Physical Acts	think, drive, ride
Physical charactrestics	red, cold, young

1.2.2 Learning Model

Learning new words and improving new vocabulary can be carried out by the following ways.

- Absorption
- Memorization
- Analysis

1.3 Analyzing words

1.3.1 Morphemes

Word analysis involves breaking a word into its morphemes. Literally morphemes means ***an element in a system of forms.***
In linugustics, it is defined as

"The smallest ***form*** which is paired with a particular ***meaning***"

From Dictionary: ***morpheme***, noun, very rare

Minimal meaningful language unit;
It cannot be divided into smaller meaningful units;

1.3.2 Characteristics of morphemes

Morphemes have four defining characteristics:

- They cannot be subdivided.
- They add meaning to a word.

- They can appear in many different words.
- They can have any number of syllables.

1.3.3 Problems with morphemes

There is no one-to-one mapping between *FORM* ↔ *MEANING*

- One form, two (or more) meanings.

  in- '*not*' in words like **in**capable and **in**sufficient, &
  in- '*into, within*', as in **in**vade and **in**clude.

- Two (or more) forms, one meaning.
  - Two (or more) forms, one meaning = two morphemes

    andr- '*man,male*' in words like **andr**oid &
    vir- '*man,male*', as in **vir**ile
  - Two (or more) forms, one meaning = one morpheme

    pan- and **pant-** , which are different forms of a Greek morpheme meaning 'all,overall'.

The alternate forms of a single morpheme are called **allomorphs**,literally 'other forms.'

1.3.4 How to analyze words

- Only Words borrowed from Classic languages like Greek and Latin can be analyzed
- Native words or words borrowed from exotice languages can not be analyzed

There are four steps as following in analyzing a word

- Parse : Divide it into its morpheme
- Gloss : Give the meaning for a morpheme
- Give a literal meaning : Use the meanings from the glosses to construct a literal meaning

- Give a dictionary definition : Extended literal meaning metaphorically to arrive at the actual meaning.

Example :

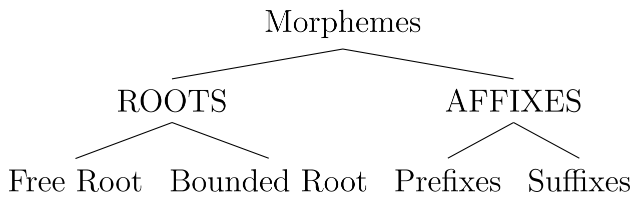
- **repellent**
- re- / pel / (l) / -ent
- 'again, back' / 'push' / (l) / A, N
- 'something which pushes back' / (l) /A,N

'A, N.' : The letters stand for 'ADJECTIVE, NOUN'

1.4 Words - their construction and use

1. How words are constructed
   (a) Types of Roots
   (b) Types of Affixes
2. How words are used - NOUNS, VERBS and ADJECTIVES

1.4.1 How words are constructed



Roots

- Roots usually have a rather specific meaning
- This meaning tends to be relatively constant across all the words that use the root.
- Roots also contribute the greatest conceptual content to the overall meaning of the word.
- Every word has at the least one root.

- Roots have freer distribution; that is, they can occur almost anywhere in a word
- Two ore more roots combine to form Compound words.
- Compound words may or may not have affixes.

Free Roots

- Free Roots are roots that can occur alone as whole words
- They can stand alone as single words.
- Free roots can also be combined with other roots or affixes to form more complex words

Bounded Roots

- Bound Roots can never occur alone as whole words.
- They cannot stand alone;
- They must occur in combination with other morphemes
- Almost all the Latin and Greek roots we are studying are bound roots

Affixes

- Affixes are morphemes which attach to roots or a combination of roots and other affixes.
- Their main use is to modify the meaning conveyed by the root or roots.
- Affixes by definition are always bound or affixed to a root.
- They are divided into two different types depending on where they attach to the root.
- Prefixes occur before a root (although several prefixes can be strung together before a single root).
- Suffixes occur after a root (although multiple suffixes can occur at the ends of words).

1.5 Suffixes and Prefixes

1. Suffixes

   (a) Inflectional suffixes

   - Add only grammatical information
   - Never change the part of speech

   (b) Derivational suffixes

   - Make a new word with a new meaning
   - Usually change the part of speech

   (c) Meanings of Derivational Suffixes

2. Prefixes

   (a) Spatial Prefixes

   - The largest group of prefixes denote relationships that occur in space.

   (b) Non-Spatial Prefixes

   - Comparative relations
   - Quantity and Size
   - Negative Prefixes
   - Intensive prefixes

2 Number-Theoretic Reference Problems

2.1 Introduction

- Security of many public-key cryptosystems dependent on intractability of the computational problems.
- A problem is tractable if its possible to solve in polynomial time.
- Problem A can be said as reducable to Problem B, if A can be solved by employing B and other finite operations ξ.
- If A $\leq_p$ B, (i.e, A is reducable to B), then A is *Computationaly Equivalent* to B, written as A $\equiv_p$ B
- If A $\equiv_p$ B, then both are tractabe or intractable.

2.2 Integer Factorization Problem

- Given a positive integer n, find its prime factors;
- Write n | $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, where p_i are pairwise primes and $e_i \geq 1$.
- A set of integers is said to be pairwise coprime if a and b are coprime for every pair (a, b) of different integers in it.

3 Cryptographic Primitives

3.1 Introduction

A symmetric or private-key cipher is one in which knowledge of the encryption key is explicitly or implicitly equivalent to knowing the decryption key.

An asymmetric or public-key cipher is one in which the encryption key is effectively public knowledge, without giving any useful information about the decryption key.

trapdoor is a computation which runs much more easily in one direction than back.

Example : Multiplication of large integers is easy, while factoring of large integers is difficult.
Merely testing large numbers for primality is easy.

3.2 RSA Cipher

1. Generate two primes, p and q, such that, atleast $> 2^{512}$ or preferably $> 2^{1024}$
2. Compute **RSA Modulus, n =p.q**
3. Choose encryption exponent, **e** > 2, **randomly.**
   Often, its **Fermats number** [A positive integer, of form, $F_n = 2^{2^n} + 1$]
   $$\text{e} = 2^{16} + 1 = 65537$$
4. Make $\boldsymbol{n}$ and $\boldsymbol{e}$ public
5. Compute decryption exponent, such that,
   $$e.d = 1 \ mod \ (p-1)(q-1)$$
6. Encryption : $E_{n,e}(x) = x^e \ \% \ n \Rightarrow y$
7. Decryption : $D_{n,d}(y) = y^d \ \% \ n \Rightarrow x$

4 Logrithms

4.1 Logarithm definition

If, a number b is raised to a power x, such that,

$$b^x = y$$

Then the base b logarithm of x is equal to y:

$$\log_b(x) = y$$

Then, we can conjure logrithms as the inverse of exponentiation, like

$$b^y = x$$

Example :

$$\begin{gathered} \log_2(32) = 5 \Rightarrow 2^5 = 32 \\ \log_2(16) = 4 \Rightarrow 2^4 = 16 \\ \log_2(8) = 3 \Rightarrow 2^3 = 8 \end{gathered}$$

4.2 Logrithms Rules

Rule	**Explanation**
Logarithm product rule	$log_b(x.y) = log_b(x) + log_b(y)$
Logarithm quotient rule	$log_b(x/y) = log_b(x) - log_b(y)$
Logarithm power rule	$log_b(x^y) = y.log_b(x)$
Logarithm base switch rule	$log_b(c) = 1/log_c(b)$
Logarithm base change rule	$log_b(x) = log_c(x)/log_c(b)$
Derivative of logarithm	$f(x) = log_b(x) \Rightarrow f^{'}(x) = 1/(xln(b))$
Integral of logarithm	$\int log_b(x)dx = x.(log_b(x) - 1/ln(b)) + C$
Logarithm of negative number	$log_b(x)$ is undefined when $x \leq 0$
Logarithm of 0	$log_b(0)$ is undefined $\lim_{x\to 0^+} \log_b(x) = -\infty$
Logarithm of 1	$log_b(1) = 0$
Logarithm of the base	$log_b(b) = 1$

5 English Syllables

Divide words based on the number of vowels: The number of syllables in a word coincide with the number of vowel sounds you hear when speaking the word.

Example : B<u>a</u> | *n<u>a</u>* | n<u>a</u>

Vovels: 'a,' 'e,' 'i,' 'o,' 'u' and 'y' are considered as vovewls, when found in the middle or at the end of a word.

Subtract 1 for each silent vowel in the word: Example : 'came' and 'gone,' 'E' is the most common silent vowel.

Consider words ending in 'le' as a vowel: Divide the word before the consonant right before the 'le'.
Example : Little would be divided lit/tle; fumble as fum/ble; able as a/ble.

Count diphthongs as 1 syllable instead of 2 : diphthongs are two vowels, combinedly giving one syllabel. Example : Words like 'h<u>au</u>l,' 'm<u>oo</u>n,' and 'c<u>oi</u>l' are diphthongs.

Split words between consonants, surrounded by vowels. Example : hap/py, din/ner, bas/ket, un/der.

Find syllables by splitting a word before a single consonant. Examples are: au/tumn, o/pen, de/tail:

Mark prefixes and suffixes as syllabels:

6 Group

A group G is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of #1 closure, #2 associativity, #3 the identity property, and #4 the inverse property.

1. Closure: If A and B are two elements in G, then the product AB is also in G.

2. Associativity: The defined multiplication is associative, i.e., for all A,B,C in G, (AB)C=A(BC).

3. Identity: There is an identity element I (a.k.a. 1, E, or e) such that IA=AI=A for every element A in G.

4. Inverse: There must be an inverse (a.k.a. reciprocal) of each element. Therefore, for each element A of G, the set contains an element B=A$\hat{(}$-1) such that AA$\hat{(}$-1)=A$\hat{(}$-1)A=I.

Group Theory: Study of groups.

Finite Group: The group has a finite number of elements.

Subgroup: A subset of group, which is *closed* under *group operation* is called as subgroup.

Cyclic Group: Cyclic group is a group, that is generated by a single element. That is,

- It consists of a set of elemnets, with single invertible assosiative operation and
- a element g, such that, every other element in the group can be obtained by applying the group operation or its inverse to g.

Cyclic group is closed under addition, associative and has unique inverse.

Homomorphism: A map between two groups, which preserve identity and group operation is called Homomorphism.

Isomorphism: If a homomorphism has an inverse which is also an homomorphism, this is called as *isomorphism* and the two group is said to be isomorphic.

7 Android Services

We will see,

1. What is a Service?
2. Service Lifecycle
3. Permissions
4. Process Lifecycle
5. Local Service Sample
6. Remote Messenger Service Sample

7.1 Introduction

A Service is an application component, representing either

- an application's desire to perform a longer-running operation while not interacting with the user. *This corresponds to calls to* ***Context.startService()***
- to supply functionality for other applications to use. *This corresponds to calls to* ***Context.bindService()***

Service is

- Not a seperate process
- Not a seperate thread

Each service class must have a corresponding <service> declaration in its package's ***AndroidManifest.xml.***
Services can be started with ***Context.startService()*** and ***Context.bindService().***

7.2 Service Lifecycle

If someone calls *Context.startService()* $\longrightarrow$ *onCreate()* $\longrightarrow$ *onStartCommand(Intent, int, int)* $\longrightarrow$ run until *Context.stopService()* or *stopSelf()* is called

START_STICKY is used for services that are explicitly started and stopped as needed.
START_NOT_STICKY or *START_REDELIVER_INTENT* are used for services that should only remain running while processing any commands sent to them.
onDestroy() method is called and the service is effectively terminated.

7.3 Permissions

Global access to a service can be enforced when it is declared in its manifest's <service> tag. By doing so, other applications will need to declare a corresponding <uses-permission> element in their own manifest to be able to start, stop, or bind to the service.
This can be bypassed by using *Intent.FLAG_GRANT_READ_URI_PERMISSION* and/or *Intent.FLAG_GRANT_WRITE_URI_PERMISSION* on the Intent, when using *Context.startService(Intent).*

7.3.1 <uses-permission>

Requests a permission that the application must be granted in order for it to operate correctly. Permissions are granted by the user when the application is installed, not while it's running.

- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.BROADCAST_STICKY
- com.sec.android.app.sysscope.permission.RUN_SYSSCOPE
- com.sec.android.app.sysscope.permission.ACCESS_SYSTEM_INFO_SYSSCOPE_ONLY

7.3.2 <permission>

Declares a security permission that can be used to limit access to specific components or features of this or other applications.

- com.sec.android.app.sysscope.permission.RUN_SYSSCOPE
  protectionLevel=dangerous
- com.sec.android.app.sysscope.permission.ACCESS_SYSTEM_INFO_SYSSCOPE_ONLY
  protectionLevel=signature
- com.verizon.permission.RECEIVE_ROOT_STATUS
  protectionLevel=signatureOrSystem

7.3.3 <permission-group>

Declares a name for a logical grouping of related permissions. Individual permission join the group through the permissionGroup attribute of the ¡permission¿ element. Members of a group are presented together in the user interface.

- permissionGroup="com.sec.android.app.sysscope.permission-group.SYSTEM_DIAGNOSIS

7.3.4 <application>

The declaration of the application. This element contains subelements that declare each of the application's components and has attributes that can affect all the components.
Many of these attributes set default values for corresponding attributes of the component elements. Others set values for the application as a whole and cannot be overridden by the components.

- android:persistent="false"
  Whether or not the application should remain running at all times

7.3.5 <receiver>

Declares a broadcast receiver as one of the application's components.
Broadcast receivers enable applications to receive intents that are broadcast by the system or by other applications, even when other components of the application are not running.

- name=".receiver.BootCompleteReceiver"
  On invocation by a broadcast, call this method.

7.3.6 <intent-filter>

Specifies the types of intents that an activity, service, or broadcast receiver can respond to.

- name="android.intent.action.BOOT_COMPLETED"
  Respond to BOOT_COMPLETED intent broadcast.

7.3.7 <service>

Declares a service (a Service subclass) as one of the application's components.

- name=".service.SysScopeService"
  The name of the Service subclass that implements the service.

- permission="com.sec.android.app.sysscope.permission.RUN_SYSSCOPE"
  The name of a permission that that an entity must have in order to launch the service or bind to it.

- intent-filter : name="com.sec.intent.action.SYSSCOPE
  Adds an action to an intent filter.

8 Two step verification :

8.1 Factors of Authentication

Factor	Explanation	Example
Ownership factor	Something that user has	ID Card, A hardware, Token
Knowledge factor	Something that user knows	Password, PIN
Inherence factor	Something that is inhere to user	Biometrics like fingerprint, retina etc

8.2 Two step verification :

For a secured and positive authentication, atleast there should be two or all three factors involve in authentication.

Single Sign On A method to authenticate in a system which has multiple secured, independent systems. By this Single Sig On, a user logins in and autheticates one system and gains acess to all the systems.

9 Newline representation :

Carriage Return [CR] : Reset typewriters horizontal position to the far left.

Line Feed [LF] : Advance the paper by one line.

ASCII Based systems

A type writer typically needs both. Windows uses CR+LF. Linux uses only LF. MAC OS, prior to OS-X used CR alone.

IBM Pc's based on EBCDIC uses a special character called as *Newline* ***[NL]***

10 Turing Machine

A Turing machine can be thought of as a primitive, abstract computer. Alan Turing, who was a British mathematician and cryptographer, invented the Turing machine as a tool for studying the computability of mathematical functions. Turing's hypothesis (also known has Church's thesis) is a widely held belief that a function is computable if and only if it can be computed by a Turing machine. This implies that Turing machines can solve any problem that a modern computer program can solve. There are problems that can not be solved by a Turing machine (e.g., the halting problem); thus, these problems can not be solved by a modern computer program.

10.1 Components of a Turing Machine

A Turing machine has

- an infinite tape that consists of adjacent cells (or squares).
- On each cell is written a symbol. The symbols that are allowed on the tape are finite in number and include the blank symbol.
- Each Turing machine has it's own alphabet (i.e., finite set of symbols), which determines the symbols that are allowed on the tape.
- a tape head that is positioned over a cell on the tape. This tape head is able to read a symbol from a cell and write a new symbol onto a cell.
- The tape head can also move to an adjacent cell (either to the left or to the right).
- A Turing machine has a finite number of states, and, at any point in time, a Turing machine is in one of these states.
- A Turing machine begins its operation in the start state.
- A Turing machine halts when it moves into one of the halt states.

10.2 Opeartion of a Turing Machine

1. The Turing machine reads the tape symbol that is under the Turing machine's tape head. This symbol is referred to as the current symbol.
2. The Turing machine uses its transition function to map the following:

   {the current state and current symbol} = {the next state, the next symbol and the movement for the tape head.}

3. The Turing machine changes its state to the next state, which was returned by the transition function.
4. The Turing machine overwrites the current symbol on the tape with the next symbol, which was returned by the transition function.
5. The Turing machine moves its tape head one symbol to the left or to the right, or does not move the tape head, depending on the value of the 'movement' that is returned by the transition function.
6. If the Turing machine's state is a halt state, then the Turing machine halts. Otherwise, repeat sub-step #1.

11 NP Complete

Decision problem : Any problem with an answer, YES or NO.

P : A decision problem that can be solved in polynomial time. That is, given an instance of the problem, the answer yes or no can be decided in polynomial time.

Example : Given a graph connected G, can its vertices be colored using two colors so that no edge is monochromatic. Algorithm: start with an arbitrary vertex, color it red and all of its neighbors blue and continue. Stop when you run our of vertices or you are forced to make an edge have both of its endpoints be the same color.

NP : A decision problem where instances of the problem for which the answer is yes have proofs that can be verified in polynomial time. This means that if someone gives us an instance of the problem and a certificate (sometimes called a witness) to the answer being yes, we can check that it is correct in polynomial time.

Example: Integer factorization is NP. This is the problem that given integers n and m, is there an integer f with 1 ¡ f ¡ m such that f divides n (f is a small factor of n)? This is a decision problem because the answers are yes or no. If someone hands us an instance of the problem (so they hand us integers n and m) and an integer f with 1 ¡ f ¡ m and claim that f is a factor of n(the certificate) we can check the answer in polynomial time by performing the division n / f.

NP-complete : An NP problem X for which it is possible to reduce any other NP problem Y to X in polynomial time. Intuitively this means that we can solve Y quickly if we know how to solve X quickly. Precisely, Y is reducible to X if there is a polynomial time algorithm f to transform instances x of X to instances y = f(x) of Y in polynomial time with the property that the answer to x is yes if and only if the answer to f(x) is yes.

Example: 3-SAT. This is the problem wherein we are given a conjunction of 3-clause disjunctions (i.e., statements of the form
(x_v11 or x_v21 or x_v31) and (x_v12 or x_v22 or x_v32) and ... and (x_v1n or x_v2n or x_v3n) where each x_vij is a boolean variable or the negation of a variable from a finite predefined list (x_1, x_2, ... x_n). It can be shown that every NP problem can be reduced to 3-SAT. The proof of this is technical and requires use of the technical definition of NP (based on non-deterministic Turing machines and the like). This is known as Cook's theorem.

What makes NP-complete problems important is that if a deterministic polynomial time algorithm can be found to solve one of them, every NP problem is solvable in polynomial time (one problem to rule them all).

NP-hard : Intuitively these are the problems that are even harder than the NP-complete problems. Note that NP-hard problems do not have to be in NP (they do not have to be decision problems). The precise definition here is that a problem X is NP-hard if there is an NP-complete problem Y such that Y is reducible to X in polynomial time. But since any NP-complete problem can be reduced to any other NP-complete problem in polynomial time, all NP-complete problems can be reduced to any NP-hard problem in polynomial time. Then if there is a solution to one NP-hard problem in polynomial time, there is a solution to all NP problems in polynomial time.

The halting problem is the classic NP-hard problem. This is the problem that given a program P and input I, will it halt? This is a decision problem but it is not in NP. It is clear that any NP-complete problem can be reduced to this one.

P = NP : This the most famous problem in computer science, and one of the most important outstanding questions in the mathematical sciences. In fact, the Clay Institute is offering one million dollars for a solution to the problem (Stephen Cook's writeup on the Clay website is quite good). It's clear that P is a subset of NP. The open question is whether or not NP problems have deterministic polynomial time solutions. It is largely believed that they do not. Here is an outstanding recent article on the latest (and the importance) of the P = NP problem: The Status of the P versus NP problem.

The best book on the subject is Computers and Intractability by Garey and Johnson. My favorite NP-complete problem is the Minesweeper problem.