Topics for Exam 2, MATH433-Summer 2013

The exam will consist mainly of the problem similar to the problems from the suggested exercises posted for the preparation to the quizzes 8-14, problems of these quizzes, and the problems similar to those solved during the class.

It is also recommended to review the exams from the previous years in the following links (except problem 4 in both sample exams, problem 8 in the first sample exam and problem 7 in the second one; however, regarding section 5.4, problems similar to those of quiz 14 will be given in the test):

http://www.math.tamu.edu/∼boas/courses/433-2009b/exam2-solution.pdf

http://www.math.tamu.edu/∼yvorobet/MATH433-2010B/Exam2solved.pdf

It does not mean the exam will consist only of the problems similar to the problems from the sources listed above but such problems will form a substantial part of it. In some problems you will be ask to give a definition or a proof of a theorem that we discussed in class. Those definitions and theorems are explicitly indicated below in the bold format (some theorems will be mentioned below as well but not in bold, in this case you just need to know how to apply them, I will not ask for the proofs).

Below are the topics for the exam. Please read carefully all items below. Then make the review topic by topic. Note that the exam will cover most of the topics below. If a specific Theorem/ Corollary/theoretical exercise is indicated in this list in the bold format it means you should be able to prove it as well. Do not put yourself in the situation that you come to the test without reviewing some of the topics. I have special office hours on Friday, July 5, between 9 a.m. and 11:30 a.m. If you struggle with a topic, do not hesitate to come to my office hours or send me an email with your concerns.

1. Finite state machine (section 2.4): to be able to determine what words are accepted by automation of acceptor type and to design an automation of transducer type with prescribed type of outputs;

2. Permutations: (sections 4.1,4.2, and the additional handout posted on
   http://www.math.tamu.edu/∼zelenko/signature.pdf):

   (a) To know how to multiply permutations and how to find inverse of a permutation;

   (b) To know how to decompose a permutation in the product of disjoint cycles, how to convert a product of (non-disjoint) cycles to the product of disjoint cycles, how to find the order of the given permutation via cycle decomposition (problems 2 in the both sample exams from the links above are good practice exercise on this topic);

   (c) To know the notion of inversion in a permutation, how to find the signature via number of inversions and via a decomposition in the product of transpositions, to know what is a signature of a cycle of given length, to know how to determine the sign of the given term in the expression for the determinant of a matrix using the notion of the signature.

3. Definition and Examples of groups (sections 4.3):

   (a) To be able **to give the definition of a group** (**Definition on page 170**). To be able to check whether a given set with a given binary operation is a group. To be able **to prove the uniqueness of the identity and of the inverse in the group based on the axioms** (**Theorem 4.3.1**).

   (b) To know what is the Cayley table of a group and to know various technique to complete a partially completed Cayley table of a group.

   (c) To know various example of groups: the symmetric group $S(n)$, the alternating group $A(n)$, the group $\mathbb{Z}_n$ (the group of congruence classes modulo n under addition), the group G_n (the group of invertible congruence classes modulo n under multiplication), various group of matrices and

transformations (the General Linear group, the Special Linear group, the orthogonal group, the special orthogonal group, the group of upper triangular matrices, the group of rigid motions, the group of symmetries of a geometric figure including the dihedral group $D(n)$ of symmetries of a regular n-sided polygon.)

4. Basic theory of groups (section 5.1, 5.2, 5.3):

   (a) To be able **to prove the cancelation property** (**Theorem 5.1.1, page 202**).

   (b) To know the notion of the subgroup and how to check weather a subset of a given group is a subgroup (using Theorem 5.1.5, page 207);

   (c) To know the notion of the order of an element, to be able to prove that **in the finite group any element has finite order** (see Example 2 page 206, where it refers to Theorem 4.2.2 for the proof of this statement in the particular situation of the symmetric group but **we discussed the proof in general case in class**); to be able to prove that **if k is an order of g and $g^n = e$, then k divides n** (we discussed it in class, see also related Theorem 5.1.4 page 205 and Theorem 4.2.3 page 161).

   (d) To be able **to give a definition of isomorphism of groups** (**Definition on pages 219 and 220**) and to know that an isomorphism preserves the order of elements. To know the notion of a cyclic group and to know that there is exactly one cyclic group of given order up to an isomorphism (basically it is Theorem 5.1.7 , we also discussed it in class). To know the notion of a cyclic subgroup generated by an element of the group. To know that any subgroup of a cyclic group is cyclic and to be able to list all subgroup of a cyclic group according to the following rule: if $G =< x >$ and has order n then all subgroup of G have the form $G =< x^d >$, where d divides n (see for example problems 5 of the sample exam from the second link above). To be able, given a generator of a cyclic group, to find all other elements that also generate it and to be able to find the orders of any other elements (see problem 2 of quiz 11).

   (e) To know the notion of left and right cosets of a subgroup and to be able to list all left or right cosets of a given subgroup. Yo know the Lagrange theorem (Theorem 5.2.3). To be able **to prove both corollaries of the Lagrange Theorem** (**Corollary 5.2.4 and Corollary 5.2.5**). To know how to apply Corollary 5.2.4 in order to find possible orders of element of the group.

   (f) To know the classification of all groups of order less or equal to 6 up to an isomorphism. In particular, given a group of order 4 to be able to determine whether it is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times Z_2$ via the analysis of the orders of the elements.

5. Error detecting and error correcting codes (part of section 5.4 as prescribed below):

   (a) To know how to deal with ISBN-10 and ISBN-13, e.g. to find a missing digit or to check the validity of these codes;

   (b) To understand the notion of a code detecting k errors and correcting k errors and how to determine this property via the notion of the distance (Theorems 5.4.1 and 5.4.2, page 236) and , in the case of linear codes, of the lowest weight of a nonzero codeword (Theorem 5.4.3, page 237). To be able to do this for a linear code if the generator matrix of the code function is given.