MATH 601 Information for Final Exam
Thursday, May 10, 2018, 7:30–10:00 am, 302 Snow Hall

The exam covers the material of the entire semester, with more emphasis on material not covered on the midterm exam. The final exam should be approximately twice as long as the midterm (but you will have three times the amount of time to do it).

You should know the statements of theorems and definitions, know how to do all the homework problems, and know the proofs listed below. You may be asked to solve and prove other things as well, at the difficulty level of homework problems.

Recommended: The Review Exercises on Converses should help you to understand the difference between a statement and its converse, and to know when both are true.

Proofs of Theorems

From the list for the midterm exam:

- The error patterns that a code C does not detect are precisely the sums $b+c$ of two codewords.
- If C is a linear code, then $d(C)$ is the minimum weight of a nonzero codeword in C.
- If C is a linear $[n,k,d]_2$ code, then $d-1 \leq n-k$.
- Let C be a linear code of length n. Then for every u, v in $\mathbf{F}^n$,
  if $u \in C+v$, then $C+u = C+v$.

New:

- The weight of any word in the extended Golay code C_{24} is a multiple of 4. You may assume that C_{24} is self-dual.
- If C is a linear code and $\{v_1, v_2, \ldots, v_k\}$ is a basis for C, then C is cyclic if and only if for all i, $\pi(v_i)$ is in C.
- The generator polynomial of a nontrivial cyclic code is unique.
- Let $g(x)$ be a polynomial in $\mathbf{F}[x]$. If the set $K = \mathbf{F}[x]/(g(x))$ with the operations of multiplication and addition mod $g(x)$ is a field, then $g(x)$ is irreducible.