Algorithms CMSC-37000 Fifth Quiz. March 8, 2007
Instructor: László Babai

Name: ______________________________

Show all your work. **Do not use book, notes, or scrap paper.** Write your answers in the space provided. When describing an algorithm in pseudocode, **explain the meaning of your variables** (in English). This quiz contributes 6% to your course grade.

1. (3+3 points) Determine (a) the minimum and (b) the maximum number of keys stored in a 2-3-4-tree (a B-tree with parameter $t = 2$) of height h. Your answers should be very simple closed-form expressions. Indicate how you got the answers.

2. (3+3+9 points) (a) Define the exact-3-cover problem (X3C). (b) Define the SUBSET-SUM problem. (c) Give a Karp-reduction from X3C to SUBSET-SUM. You only need to give the reduction; don't prove correctness.

3. (3+8+8 points) (a) Define the language FACT which corresponds to the decision version of the factoring problem for integers. (b) Prove that FACT belongs to coNP, assuming the set of prime numbers, PRIMES, belongs to NP. Do not assume the AKS theorem that PRIMES belongs to P. (c) Explain why we believe that FACT is not NP-complete. State and prove the unexpected consequence that the NP-completeness of FACT would have.

4. (3+4+6+7+8B points) (a) Define what it means for a family $\mathcal{H}$ of hash functions $h : U \to \{0, 1, \dots, n-1\}$ to be universal. (b) Let $S \subset U$ have n elements. Pick $h \in \mathcal{H}$ at random. Let X denote the number of collisions in S, i. e., the number of unordered pairs $\{u, v\} \subset S$ such that $u \neq v$ but $h(u) = h(v)$. Give a tight upper bound on $E(X)$. Prove. (c) Let p be a prime, $r \geq 1$. Let $N = p^r$ and $n = p$. Construct the universal family of N hash functions over a universe of size N as discussed in class. (d) Prove the universality of your family of hash functions. (e) BONUS: Let S be a linearly independent subset of the vector space U constructed in part (c). Prove: $\mathrm{Var}(X) < E(X)$.