Meeting: 1007, Santa Barbara, California, SS 10A, Special Session on Complexity of Computation and Algorithms

1007-68-26 **Christopher J Pollett*** (cpollett@yahoo.com), Dept. of Computer Science, San Jose State University, One Washington Square, San Jose, CA 95192, and **Norman Danner**, Dept. of Mathematics and Computer Science, Wesleyan University, Middletown, CT 06549. *Circuit Principles and Weak Pigeonhole Variants.*

This talk considers the relational versions of the surjective and multifunction weak pigeonhole principles for various classes of formulas. These principles are interesting because of their close connection to the provability of circuit lower bounds, and hence the P versus NP question, in weak systems of arithmetic. We show that the relational surjective pigeonhole principle for Θ^b_2 formulas in S^1_2 implies a circuit block-recognition principle which in turn implies the surjective weak pigeonhole principle for Σ^b_1 formulas. We introduce a class of predicates corresponding to poly-log length iterates of polynomial-time computable predicates and show that over R^1_2, the multifunction pigeonhole principle for such predicates is equivalent to an "iterative" circuit block-recognition principle. A consequence of this is that if R^2_3 proves this circuit iteration principle then RSA is vulnerable to quasi-polynomial time attacks. (Received December 11, 2004)