**MURRAY R. BREMNER**, University of Saskatchewan

*Computing a short basis for the nullspace of a modular matrix*

Given a vector $X$ over the field with $p$ elements, define its length to be the sum of the squares of the symmetric representatives of its components. Define the length of a finite set of vectors to be the base 10 logarithm of the product of the lengths of the vectors. I will present an evolutionary algorithm which attempts to determine the shortest basis of the nullspace of a modular matrix $A$. To begin, compute $M$, the matrix in RREF whose $k$ rows form a basis for the null space of $A$. One generation consists of six steps. Step 1 (mutation): Randomly permute the columns of $A$ to obtain $B$. Step 2: Compute $C$, the matrix in RREF whose $k$ rows form a basis for the null space of $B$. Step 3: Unpermute the columns of $C$ to obtain $N$. Step 4 (recombination): Stack $M$ and $N$ and sort the $2k$ rows by increasing length to obtain $D$. Step 5 (selection): Determine the lexicographically minimal subset of the rows of $D$ which forms a basis of the nullspace of $A$. Step 6 (reproduction): Replace $M$ by the matrix consisting of these $k$ rows of $D$. I will present experimental results showing the behavior of this algorithm over thousands of generations.