Squaring square matrices

Take-home SMV problem, April 18, 2011

Deadline for solutions: May 9, 2011

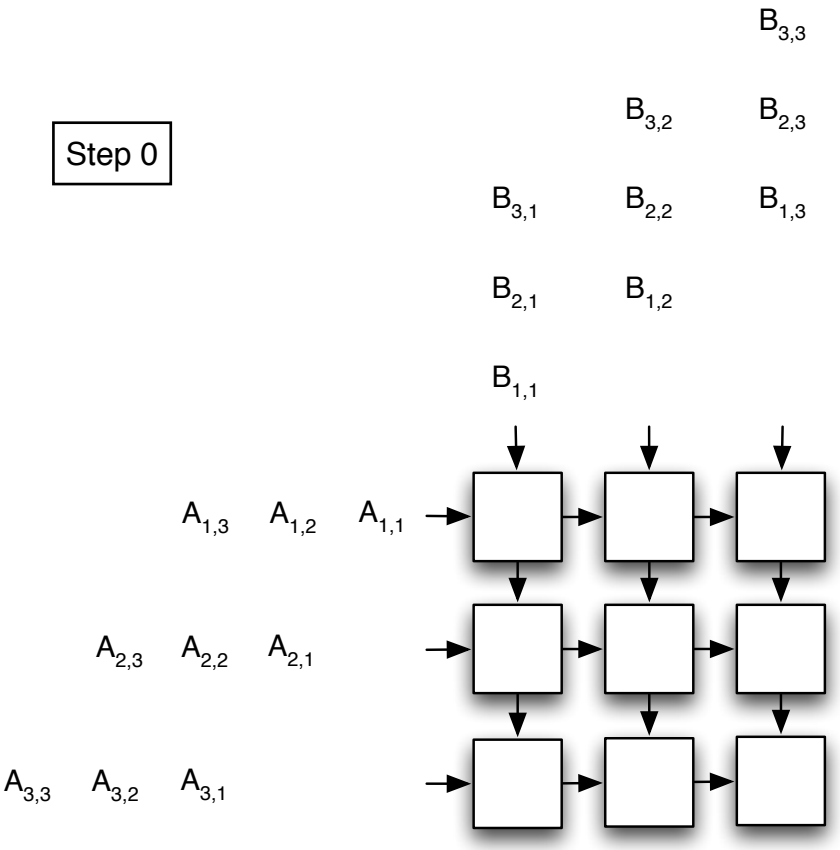
1. **Introduction**

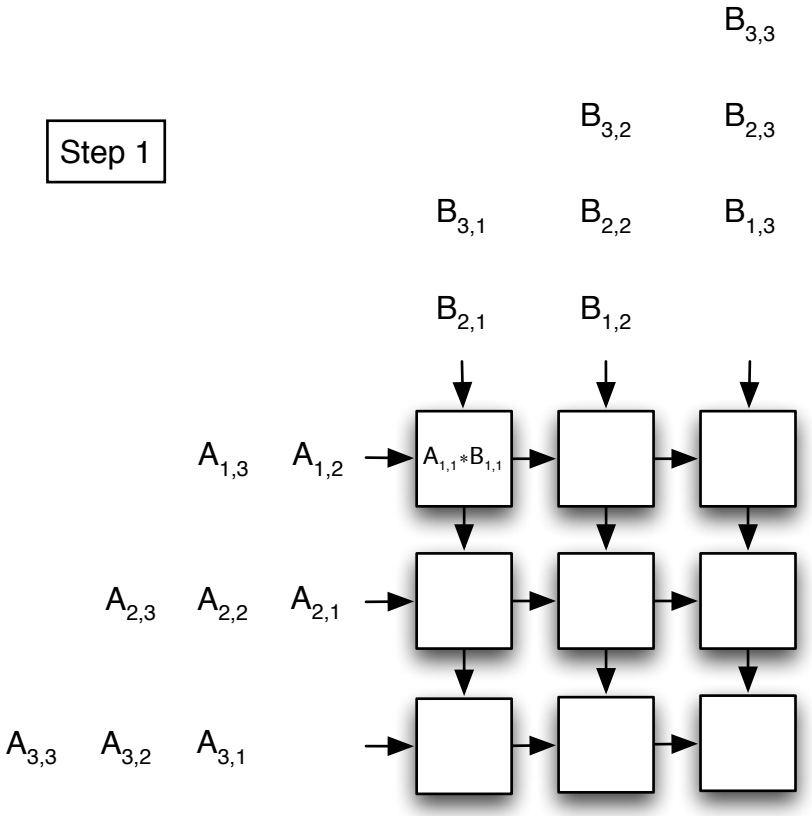
Your task is to model a network that can store square binary matrices and square them (i.e., multiply them by themselves)

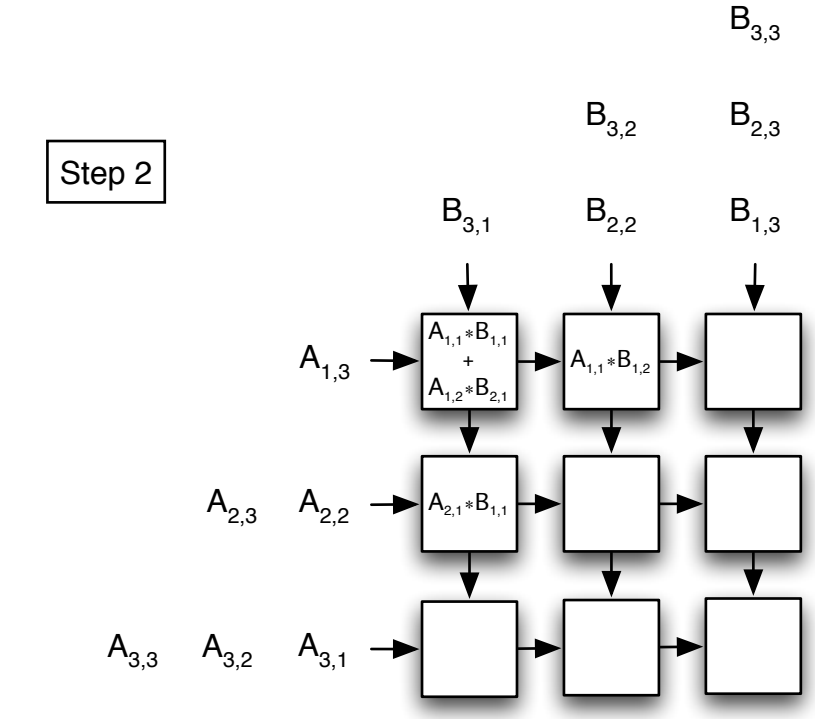
To multiply square matrices on a parallel machine:

$$\begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,1} & A_{3,2} & A_{3,3} \end{bmatrix} \quad \begin{bmatrix} B_{1,1} & B_{1,2} & B_{1,3} \\ B_{2,1} & B_{2,2} & B_{2,3} \\ B_{3,1} & B_{3,2} & B_{3,3} \end{bmatrix}$$

one can use a square network of processors that succesively get rows and columns of the two (suitably turned and skewed) matrices. The following diagrams illustrate the first steps of such a network:



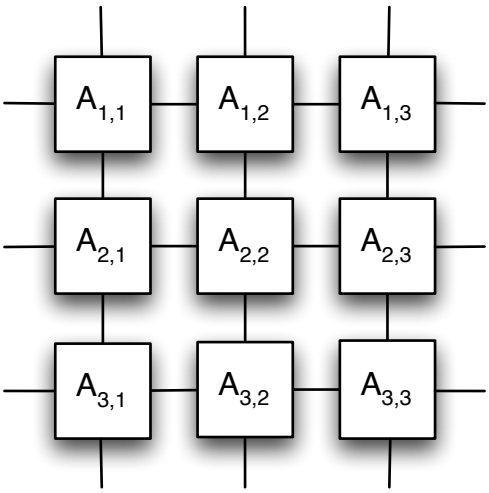




..etc. As a result, after 3n-2 steps, the network stores the product of the two matrices.

2. Task

Write an SMV module that can store a binary matrix (i.e., a matrix over the two-element field Z_2) of size NxN, in a network of cells:



and uses the parallel algorithm described above to square the stored matrix (i.e., to multiply it by itself) in a linear number of steps.

Then, using any SMV verification techniques you find convenient, for two different N>1 perform the following tasks:

1) Find a matrix with more than N 1's that, when squared, becomes the identity matrix (i.e. a matrix with all 1's on the diagonal and all 0's elsewhere), or prove that such matrices do not exist,

2) Prove that every matrix with all 0's on the diagonal and below the diagonal is nilpotent, i.e., that after getting squared sufficiently many times it becomes the zero matrix,

Try to do these tasks for N as large as you can.

2. **Emergency version (for half the score)**

If the above problem seems too hard, then try to model a system that stores square matrices and squares them in any way you can, not necessarily in a linear number of steps with a network of cells. But, in addition to the two tasks listed above:

3) Find a matrix that has some 1's beside the diagonal and that, when squared, becomes itself again, or prove that such matrices do not exist.