Matrix multiplication and pattern matching under Hamming norm

Raphaël Clifford

January 23, 2009

Abstract

My understanding of a conversation with Ely Porat who in turn attributes Piotr Indyk.

1 Reduction

We want to show a reduction from binary matrix multiplication of some sort to pattern matching under the Hamming norm.

Consider the following reduction. Assume the input is of two binary matrices A and B of sizes $m \times \ell$ and $\ell \times n$. For matrix A, we write x for each 0 and for each 1 we write its column number. For example, $A = ((0, 0, 1), (1, 0, 1))$ is translated to $A' = ((x, x, 3), (1, x, 3))$. For matrix B, we write y for each 0 and the row number for each 1. For example, $B = (0, 1), (1, 0), (0, 0))$ is translated to $B' = ((y, 1), (2, y), (y, y))$. Now create pattern p as the concatenation of the rows of A' and text t as the concatenation of the columns of B' with the unique symbol \$ inserted after every column and add $\ell(m-1)$ \$ symbols at the beginning and end of t. So, in our example $p = xx31x3$ and $t = \$\$\$y2y\$12y\$\$\$$.

We now count the number of matches between p and t at each alignment, giving in this case $0, 0, 0, 0, 1, 0, 0, 0, 0, 0$ meaning that the second row of A scored 1 when multiplied with the second column of B. The trick is that the \$ symbols force at most one substring of the pattern corresponding to a row in A to match one substring of t corresponding to a column of B at any given alignment.