A quick intro to Knuth's Algorithm

December 9, 2009

1 Introduction

Here we consider the following problem.

Problem. Find integers x and y such that

$$5x + 13y \ = \ \gcd(5, 13) \ = \ 1.$$

2 The basic Knuth algorithm

To solve this we begin by forming the matrix

$$\left[\begin{array}{ccc} 1 & 0 & 5 \\ 0 & 1 & 13 \end{array}\right].$$

The first column represents the coefficients of 5, the second column represents the coefficients of 13, and the last column represents a linear combination of 5 and 13 determined by these coefficients. For example, if the first column had entries a, a', and the second column had entries b, b', then the matrix would look like

$$\left[\begin{array}{ccc} a & b & 5a + 13b \\ a' & b' & 5a' + 13b' \end{array}\right].$$

Now we perform a sequence of "row operations" (just like with Gaussian elimination) to convert the third column into one whose entries are 0 and $g = \gcd(u, v)$, where $u = 5$ and $v = 13$ in our case. **But unlike with Gaussian elimination, the types of operations we can do are constrained to the following:**

- We can add an **integer** multiple of one row to another, leaving the row unchanged whose multiple we added to the other.
- We can interchange two rows.
- We can multiply a row by an **integer** multiple.

The goal is to make the numbers in the right column smaller, until we get down to 0 and g. So, let us perform some row operations on the above matrix to find x and y:

$$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 13 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 5 \\ -2 & 1 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & -1 & 2 \\ -2 & 1 & 3 \end{bmatrix}$$
$$\rightarrow \begin{bmatrix} 3 & -1 & 2 \\ -5 & 2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 13 & -5 & 0 \\ -5 & 2 & 1 \end{bmatrix}.$$

Let's discuss: In the first step we multiplied row 1 by -2 and then added the resulting row vector to row 2; then, we multiplied row 2 by -1 and added the result to row 1; etc.

Notice we reached a row with 1 as the right-most entry, namely the row with entries $-5, 2$, and 1. This row corresponds to the relation

$$5x + 13y \;=\; 5 \cdot (-5) + 13 \cdot 2 \;=\; 1.$$

So, $x = -5$ and $y = 2$ is the solution we sought.

Also notice that we could actually have backed out one step earlier – that last step with right-most column $[0\ 1]^{\text{transpose}}$ was really unnecessary, since we got the $-5, 2, 1$ row in the previous iteration. In general, it is a good idea to iterate all the way, but if you can spot that you already have the relation you need, then you can stop the algorithm early and report the results.