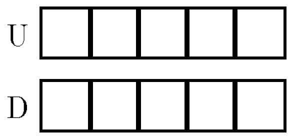
A Note on Bryant's Proof of Exponential Lower Bound for Multiplication

Alan J. Hu
for CpSc 513
Univ. of British Columbia

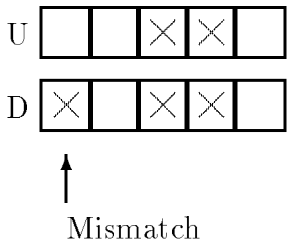
September 18, 1997

One of the central arguments in the proof is that we are always guaranteed to be able to find $n/8$ inputs split by the partition. I believe it is easier to understand this argument if we pull it out from the multiplication proof and consider it separately.

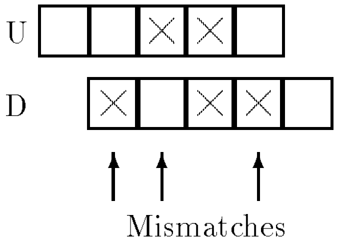
Consider a game played with two sticks U and D, each made up of m squares:



Your opponent marks half of the squares (m total marked squares out of the $2m$ squares on both sticks):



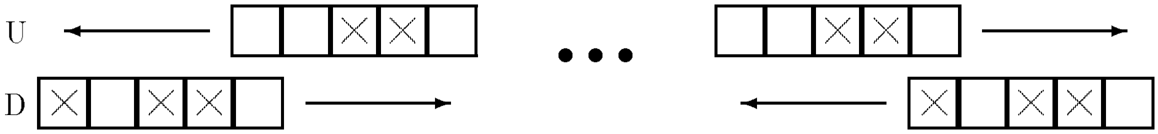
If you line up the two sticks, define a **mismatch** as having a marked square on one stick lined up with an unmarked square on the other. For example, in the above marking and alignment, we have only one mismatch. You win the game if you can find a way to line up the sticks such that you have at least $m/4$ mismatches. For example, if we slide the lower stick D one square to the right, we get 3 mismatches:



Since $m = 5$ in this example, and $3 > 5/4$, you win.

We will now prove that you can always win this game.

Proof: There are $2m - 1$ ways to line up the two sticks:



If we consider all possible ways to line up the two sticks, each square in D gets lined up with each square in U in exactly one alignment. Thus, if we add up the number of mismatches in all $2m - 1$ possible alignments, it will equal the total number of possible mismatches, which is equal to:

$$(\#\text{ marked in } U)(\#\text{ unmarked in } D) + (\#\text{ unmarked in } U)(\#\text{ marked in } D).$$

If we let k denote the number of marked squares in U, then $m - k$ is the number of unmarked squares in U. Also, since we know our opponent had to mark exactly m squares total, we also know that $m - k$ squares are marked in D, so we also know that k squares are unmarked in D.

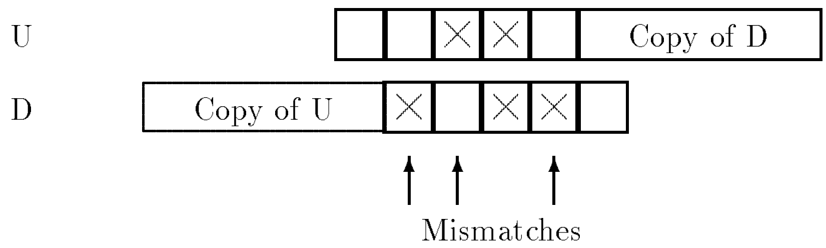
In other words, we have:

$$\begin{aligned} \sum_{\text{all } 2m-1 \text{ alignments}} (\#\text{ of mismatches}) &= k^2 + (m-k)^2 \\ &\geq m^2/2 \quad (\text{use calculus: } k = m/2 \text{ minimizes}). \end{aligned}$$

Therefore, we know that on average, an alignment will have at least $m^2/2(2m-1)$ mismatches (total number of mismatches divided by total number of alignments), which is greater than $m^2/2(2m)$, which equals $m/4$.

Since the "average" alignment must have at least $m/4$ mismatches, there must be an alignment that produces at least $m/4$ mismatches. (If every alignment produced fewer than $m/4$ mismatches, the average would have to be less than $m/4$.) This completes the proof. $\square$

To convert this back to Bryant's proof, first note that we can glue an extra copy of D on the right end of U and an extra copy of U on the left end of D.



We completely ignore the extra copies and play the game as before. In particular, we don't count "mismatches" between the original part of a stick and the extra copy glued on.

The sticks (with the glued-on extension) correspond to the two partial products formed from Operand A. U corresponds to the high-order half of A, and D is the low-order half of A. The squares correspond to input bits in A. Marked squares correspond to input bits in the L partition, and unmarked squares correspond to inputs bits in the R partition. Mismatches, therefore, are bits from the two half words that are lined up for addition, but are split between the two partitions. The embedded words U and V in Bryant's proof are the bits that are in the overlap of the **original** sticks, not including the glued-on extension.

Bryant uses n to denote the length of the stick including the extra copy, so $m = n/2$. Therefore, the lower bound on the number of mismatches becomes $n/8$.