Quantum Computing Assignment 1

Brennan W. Fieck

January 23, 2017

Problem A1. For the Turing machine model described in class that used the unary representation of numbers:

(a) How many steps of the program are needed to find $1 + 2 = 3$?

(b) How many steps of the program are needed to find $3 + 4 = 7$?

(c) How many steps of the program do you expect are required to find $n + m$ for positive integers n and m? Provide a short explanation.

Solution.

(a) Assuming the 1 is read first, 8

(b) Assuming the 3 is read first, 17

(c) It takes one step to move to the first digit of the first number, n steps to read the first number n, $3\times m$ steps to copy the second number m into the space adjacent to n and one extra step to halt computation. So the total number of steps is $n+1+3m+1 = 3m+n+2$

$\square$

Problem A2. Construct AND and OR gates from NAND and FANOUT.

Solution.

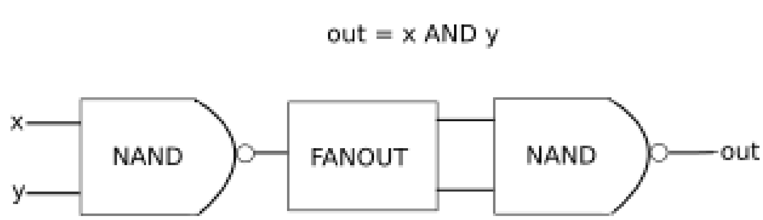

Figure 1: AND

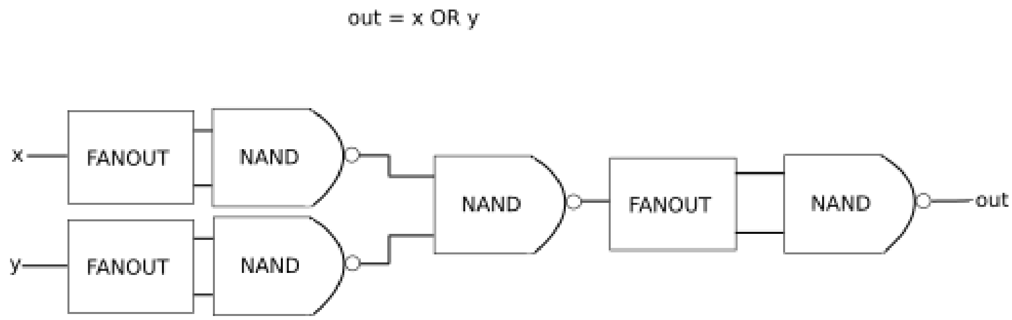

Figure 2: OR

□

Problem A3. The r^{th} roots of unity are given by $\omega_k = e^{2\pi i k/r}$ with $k = 0, 1, \ldots, r-1$

(a) Verify this statement, and give a brief geometric description of the location of the roots in the complex plane for $r = 3$.

(b) Find the sum $\sum_{k=0}^{r-1} \omega_k^n$ both when r divides n $(r|n)$ and when r does not divide n. Hint: remember to take examples as need be!

Solution.

(a) If the r^{th} roots of unity really are given by ω_k, then it must be true that $\omega_k^r = 1$.

$$\omega_k^r = (e^{2piik/r})^r = e^{2\pi i k}$$

Via Euler's Formula, it is known that for integral k, $e^{2\pi i k} = 1$. (The only reason $0 \leq k < r$ is to avoid repeat answers). Thus it must be true that ω_k represents the r^{th} roots of unity.

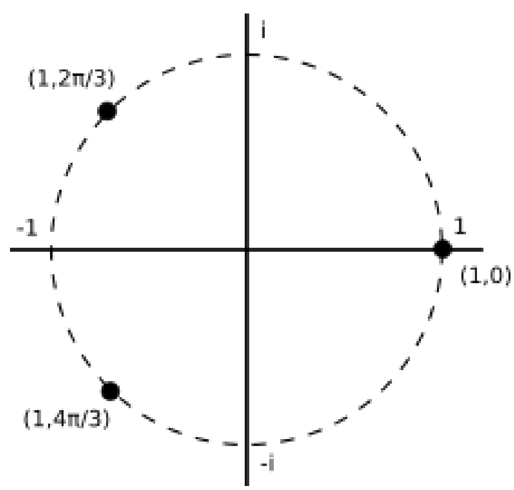

Figure 3: 3^{rd} Roots of Unity

(b) If r divides n, then let $a = n/r$, and we know that a must be positive and integral (because I assume n and r are positive and integral). Then we can write the sum:

$$\sum_{k=0}^{r-1} [\omega_k^n] = \sum_{k=0}^{r-1} \left[(e^{\frac{2\pi i k}{r}})^n \right] = \sum_{k=0}^{r-1} \left[e^{2\pi i k a} \right].$$

In this case, for any k each term in the sum is equal to 1. Thus the final value of the sum is equal to the number of terms, which is to say:

$$\sum_{k=0}^{r-1} [\omega_k^n] = r$$

. In the case that r does not divide n, $a = n/r$ will still be positive (because I still assume positive and integral n and r), but not necessarily integral. Most generally, each term ω_k^n in the sum can be written as

$$e^{2\pi i k a} = \cos[2\pi k n/r] + i \sin[2\pi k n/r]$$

using Euler's Formula. This can be separated into two sums, one over a Cosine and the other over a Sine. Fortunately, these are well-known sums that can be looked up:

$$\sum_{k=0}^{m} [\cos[2\pi a k]] = \csc[\pi a] \sin[\pi a(m+1)] \cos[\pi a m]$$

$$\sum_{k=0}^{m} [\sin[2\pi a k]] = \csc[\pi a] \sin[\pi a(m+1)] \sin[\pi a m].$$

In this case, $m = r - 1$. Thus, the original sum can be expressed:

$$\sum_{k=0}^{r-1} [\omega_k^n] = \csc[\pi a] \sin[\pi a(r-1+1)] \left(\sin[\pi a(r-1)] + \cos[\pi a(r-1)]\right)$$

or, in terms of only the given variables:

$$\csc\left[\frac{\pi n}{r}\right] \sin[\pi n] \left(\sin\left[\pi n \left(1 - \frac{1}{r}\right)\right] + \cos\left[\pi n \left(1 - \frac{1}{r}\right)\right] \right).$$

However, I prefer to simply recognize that for integral n this is just 0 because $\sin[\pi n] = 0$ for integral n.

$\square$

Problem A4. Consider a real and symmetric matrix nxn matrix A.

(a) Show that necessarily A^2 is also symmetric.

(b) The satisfaction of how many independent conditions will ensure that $A^2 = I_n$, the nxn identity?

(c) Work out the details for the entries of A for the $n = 2$ case.

Solution.

(a) If A^2 is symmetric, it must be true that $(A^2)^{\mathrm{T}} = A^2$ From the definition of a symmetric matrix, $A = A^{\mathrm{T}}$. This is useful, since we can distribute a transpose to components of matrix multiplication like so:

$$(A^2)^{\mathrm{T}} = (AA)^{\mathrm{T}} = A^{\mathrm{T}}A^{\mathrm{T}} = AA = A^2.$$

Since A^2 is equal to its transpose, it must be symmetric.

(b) Because the matrix is symmetric, satisfaction of the upper-triangular sub-matrix guarantees satisfaction of the lower-triangular sub-matrix. Thus the only *independent* conditions that need be satisfied are those on the diagonal, plus each entry to the left or right of each diagonal entry. On the m^{th} row of A^2 there are $n-m$ entries (0-indexed). This renders the sum:

$$\sum_{m=0}^{n-1}[n-m] = n^2 - \frac{1}{2}(n-1)(n-1+1) = n^2 - \frac{n(n-1)}{2}$$

$$= n^2 - \frac{n^2}{2} + \frac{n}{2} = \frac{n(n+1)}{2}$$

which is the number of independent of conditions to satisfy in order for $A^2 = I_n$.

(c) Let the matrix A be represented by

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then the entries of A^2 must be:

$$A^2 = \begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{bmatrix}.$$

For this to be I_2, the entries of A^2 therefore have the following restrictions:

$$a^2 + bc = 1$$

$$b(a+d) = 0$$
$$c(a+d) = 0$$
$$d^2 + bc = 1$$

From either of the middle two we can extract that $a + d = 0 \to a = -d$ or $b = 0$ and $c = 0$. Let's demand that $b = 0$, because we have to start somewhere or progress can't be made. In that case, the top and bottom equations dictate that $a^2 = d^2 = 1 \to a =$

± 1 and $d = \pm 1$. Since A is symmetric, $b = 0 \to c = 0$. In this case, we have four possible matrices for A:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ or } \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

On the other hand, if we demand that $a + d = 0 \to a = -d$, but that $c = d$ is not necessarily 0, then as long as the relations $a = \pm\sqrt{1 - bc}$ and $d = \mp\sqrt{1 - bc}$ are satisfied, $A^2 = I_2$ will hold. Of course, since A is symmetric, it's true that $b = c$. So, in terms of just b, A can take on the following forms:

$$A = \begin{bmatrix} \sqrt{1-b^2} & b \\ b & -\sqrt{1-b^2} \end{bmatrix} \text{ or } \begin{bmatrix} -\sqrt{1-b^2} & b \\ b & \sqrt{1-b^2} \end{bmatrix}$$

which are valid for any real value of b[1].

$\square$

[1] Actually I think this works for complex b, but I can't prove it.