Quantum Algorithms
Homework 4 Solutions

Patrick Canny

Due: 2019-02-26

1 Book Problems

1. Exercise 6.2

SOLUTION

Claim 1.1. *There is a unique linear map* $C = A \otimes B : \mathcal{L} \otimes \mathcal{M} \to \mathcal{L}' \otimes \mathcal{M}'$ *where* $C(u \otimes v) = A(u) \otimes B(v)$ *for any* $u \in \mathcal{L}, v \in \mathcal{M}$.

Proof of claim. This problem seems closely tied with the universality principle for bilinear functions. We just need to find a way to convert this problem into a problem that can utilize the universality principle. This principle states that there is a unique linear function $G : \mathcal{L} \otimes \mathcal{M} \to \mathcal{F}$ such that $F(u, v) = G(u \otimes v)$ where F is the original bilinear function.

From here we will try to create the universality function from the pieces of the problem. Let $\mathcal{F} = \mathcal{L}' \otimes \mathcal{M}'$. Then, we will define functions in the context of this $\mathcal{F}$. Take $F : \mathcal{L} \times \mathcal{M} \to \mathcal{F}$ and $F(u, v) = A(u) \otimes B(v)$.

From here, if we subsititute our newly defined properties into G from the universality principle, we can see that we have formed a unique C that aligns with the properties required by C. Since the universality function notes that this function is unique, it holds that C is also unique. •

2 Additional Problems

1. For each of the following values of q, generate 5 random members of $\{1, \ldots, q-1\}$ and run the Miller-Rabin test using them. What is the probability that q is prime?

   I suggest using python as a calculator to solve these problems. You need not show the work required to exponentiate numbers.

SOLUTION

Here is my Python implementation of the Miller-Rabin Primality Test:

```
# Patrick Canny
# EECS 700 H4
# Miller-Rabin Primality Test Implementation

import os
import math
import random

def miller_rabin(q):
    # if q even != 2 then composite
    if(q % 2 == 0):
        if (q == 2):
            return ”Prime”
        return ”Composite”
    else:
        r = 0
        s = q-1
        while s % 2 == 0:
            r += 1
            s //= 2
        for _ in range(5):
            a = random.randrange(2, q-1)
            x = pow(a, s, q)
            if x != 1:
                i = 0
                while (x != q-1):
                    if i == r-1:
                        return ”Composite”
                    else:
                        i += 1
                        x = (x ** 2) % q
        return ”Prime”

print(”Ex 1: {}”.format(miller_rabin(10601)))
print(”Ex 2: {}”.format(miller_rabin(101101)))
print(”Ex 3: {}”.format(miller_rabin(15841)))
```

(i) $q = 10601$: “Prime” (Probability $= 1$)

(ii) $q = 101101$: “Composite” (Probability $\geq 1/2$)

(iii) $q = 15841$: “Composite” (Probability $\geq 1/2$)

2. Let $\mathbb{V}$ and $\mathbb{S}$ be vector spaces over $\mathbb{C}$ with bases $\mathcal{B}_{\mathbb{V}}$ and $\mathcal{B}_{\mathbb{S}}$, respectively. Define

$$\mathbb{V} \times \mathbb{S} = \big\{(v, s) \mid v \in V \text{ and } s \in S\big\}$$

and recognize it as a vector space by *coordinate-wise* interpretation of the vector space axioms. That is,

$$\begin{aligned} (v_1, s_1) + (v_2, s_2) &= (v_1 + v_2, s_1 + s_2) && \text{for } v_1, v_2 \in V \text{ and } s_1, s_2 \in S, \\ \lambda \cdot (v_1, s_1) &= (\lambda \cdot v_1, \lambda \cdot s_1) && \text{for } v_1 \in V, s_1 \in S, \text{ and } \lambda \in \mathbb{C} \text{ a scalar.} \end{aligned}$$

If $R : \mathbb{A} \to \mathbb{V}$ and $T : \mathbb{A} \to \mathbb{S}$ are linear functions, then we can define a linear function $(R \times T) : \mathbb{A} \to \mathbb{V} \times \mathbb{S}$ by

$$(R \times T)a = \big(Ra, Ta\big) \qquad \text{for } a \in A.$$

(i) Let

$$\mathcal{C} = \big\{(b_v, b_s) \mid b_v \in \mathcal{B}_{\mathbb{V}} \text{ and } b_s \in \mathcal{B}_{\mathbb{S}}\big\}.$$

Show that $\mathbb{C}$-span$(\mathcal{C}) = \mathbb{V} \times \mathbb{S}$ but that $\mathcal{C}$ is *not* a basis for $\mathbb{V} \times \mathbb{S}$.

SOLUTION

Consider an element in $\mathbb{C}$-span($\mathcal{C}$). This element is some $\lambda_i * c_i$ given that $\lambda_i \in \mathbb{C}$ and $c_i \in \mathcal{C}$. This is also to say that this element can be written as $\lambda_i * (b_v, b_s)$ by the definition of $\mathcal{C}$. By the distributive property, this also can be expressed as the form $(\lambda_i * b_v, \lambda_i * b_s)$. This implies that we could have a number of the same element of $\mathcal{B}_{\mathbb{V}}$ or $\mathcal{B}_{\mathbb{S}}$ in a corresponding representation in $\mathbb{V} \times \mathbb{S}$. From here, we can represent an element of $\mathbb{V} \times \mathbb{S}$ as a linear combination of elements from $\mathcal{C}$ showing that $\mathbb{C}$-span($\mathcal{C}$) $= \mathbb{V} \times \mathbb{S}$

Showing that $\mathcal{C}$ is not a basis for $\mathbb{V} \times \mathbb{S}$ requires showing that either the elements of $\mathcal{C}$ are not linearly independant, or that the elements of $\mathcal{C}$ cannot compose all the elements of $\mathbb{V} \times \mathbb{S}$. The elements from $\mathcal{C}$ are all multiplied by scalars in their linear combinations that form $\mathbb{V} \times \mathbb{S}$, which would mean that the scalar multiple could be changed from say k to $2k$, meaning that there would be multiple ways to make the 0 vector, proving that $\mathcal{C}$ cannot be a basis.

(ii) Prove that

$$\mathcal{B}_{\mathbb{V}\times\mathbb{S}} = \big\{(b_v, 0), (0, b_s) \mid b_v \in \mathcal{B}_{\mathbb{V}} \text{ and } b_s \in \mathcal{B}_{\mathbb{S}}\big\}$$

is a basis for $\mathbb{V} \times \mathbb{S}$. What is the dimension of $\mathbb{V} \times \mathbb{S}$?

SOLUTION

Claim 2.1.

$$\mathcal{B}_{\mathbb{V}\times\mathbb{S}} = \big\{(b_v, 0), (0, b_s) \mid b_v \in \mathcal{B}_{\mathbb{V}} \textit{ and } b_s \in \mathcal{B}_{\mathbb{S}}\big\}$$

is a basis for $\mathbb{V} \times \mathbb{S}$.

Proof of claim. We need to show that all elements of $\mathbb{V} \times \mathbb{S}$ can be represented as a linear combination of the elements of this given basis. The elements of the basis are definitely linearly independant, as there is only one single way to produce the 0 vector (multiply each basis element by 0).

To show that all the linear combinations can be created, we can start with the fact that we can build the entire basis for both $\mathbb{S}$ and $\mathbb{V}$ by adding $0 * (b_v, 0)$ or $0 * (0, b_s)$ to all the other vectors that can be generated by choosing b_v, b_s. It is now possible to build all vectors that belong to $\mathbb{S}$ and $\mathbb{V}$, so building the vectors in $\mathbb{V} \times \mathbb{S}$ is just a matter of creating linear combinations of the vectors that fill $\mathbb{V}$ or $\mathbb{S}$. This implies that the size of $\mathbb{V} \times \mathbb{S}$ is the size of $\mathbb{V}$ times the size of $\mathbb{S}$ •

(iii) Let $R : \mathbb{A} \to \mathbb{V}$ and $T : \mathbb{A} \to \mathbb{S}$ be linear functions. Suppose that $\mathbb{A}$, $\mathbb{V}$, and $\mathbb{S}$ have ordered bases

$$\mathcal{B}_{\mathbb{A}} = \big\{a_1, a_2\big\}, \qquad \mathcal{B}_{\mathbb{V}} = \big\{v_1, v_2, v_3\big\}, \qquad \mathcal{B}_{\mathbb{S}} = \{s_1, s_2\},$$

and that the matrix representations of R and T relative to these bases are

$$(R)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{V}}} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix} \qquad \text{and} \qquad (T)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{S}}} = \begin{bmatrix} -1 & 2 \\ 3 & -2 \end{bmatrix}.$$

Using the lexicographic order for the basis $\mathcal{B}_{\mathbb{V}\times\mathbb{S}}$ (i.e. ordering by $\mathcal{B}_{\mathbb{V}}$ first, and then $\mathcal{B}_{\mathbb{S}}$), find the matrix representation for $(R \times T)$ (that is, find $(R \times T)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{V}\times\mathbb{S}}}$).

SOLUTION

To find $(R \times T)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{V}\times\mathbb{S}}}$, we seek to build a new matrix:

$$(R \times T)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{V}\times\mathbb{S}}} = \begin{bmatrix} (T)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{S}}} \\ (R)_{\mathcal{B}_{\mathbb{A}}\to\mathcal{B}_{\mathbb{V}}} \end{bmatrix} = \begin{bmatrix} -1 & 2 \\ 3 & -2 \\ 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$$

3. Let $\mathbb{V}$ and $\mathbb{S}$ be vector spaces over $\mathbb{C}$ with bases $\mathcal{B}_{\mathbb{V}}$ and $\mathcal{B}_{\mathbb{S}}$, respectively.

(i) Prove that

$$\mathcal{B}_{\mathbb{V}\otimes\mathbb{S}} = \left\{ b_v \otimes b_s \mid b_v \in \mathcal{B}_{\mathbb{V}} \text{ and } b_s \in \mathcal{B}_{\mathbb{S}} \right\}$$

is a basis of $\mathbb{V} \otimes \mathbb{S}$. What is the dimension of $\mathbb{V} \otimes \mathbb{S}$?

SOLUTION

Claim 2.2. *The above assertion is true.*

Proof of claim. Recall that to prove something is a basis, we need to show that there is exactly one way to build the 0-vector, and that all vectors in the final vector space can be represented as linear combinations of the elements of the basis.

First, let's write a compnenent of $\mathbb{V} \otimes \mathbb{S}$:

$$\sum_{i,j} a_{ij} u_i \otimes v_j$$

where $u_i, v_j \in \mathcal{B}_u, \mathcal{B}_v$ respectively. This form holds for all the members of $\mathbb{V} \otimes \mathbb{S}$. But $u_i \otimes v_j \in \left\{ b_v \otimes b_s \mid b_v \in \mathcal{B}_{\mathbb{V}} \text{ and } b_s \in \mathcal{B}_{\mathbb{S}} \right\}$. Since the elements of $\mathbb{V}\otimes\mathbb{S}$ can be expressed as linear combinations of the basis described above, this fact implies that the claim holds.

The only a_{ij} that could produce the 0-vector would be 0 itself.

•

The dimension of $\mathbb{V} \otimes \mathbb{S}$ is given by $dim(\mathbb{V}) * dim(\mathbb{S})$

(ii) Let $R : \mathbb{V} \to \mathbb{A}$ and $T : \mathbb{S} \to \mathbb{B}$ be linear functions. Suppose that $\mathbb{A}$, $\mathbb{V}$, and $\mathbb{S}$ have ordered bases the same as in the previous question and that $\mathbb{B}$ has ordered basis $\mathcal{B}_{\mathbb{B}} = \left\{ b_1, b_2 \right\}$ and that the matrix representations of R and T relative to these bases are

$$(R)_{\mathcal{B}_{\mathbb{V}} \to \mathcal{B}_{\mathbb{A}}} = \begin{bmatrix} -1 & 2 & -1 \\ 3 & -2 & -1 \end{bmatrix} \qquad \text{and} \qquad (T)_{\mathcal{B}_{\mathbb{S}} \to \mathcal{B}_{\mathbb{B}}} = \begin{bmatrix} -2 & 1 \\ 1 & -2 \end{bmatrix}.$$

Using the lexicographic order for the basis $\mathcal{B}_{\mathbb{V}\otimes\mathbb{S}}$, find the matrix representation for $(R \otimes T)$ (that is, find $(R \times T)_{\mathcal{B}_{\mathbb{V}\otimes\mathbb{S}} \to \mathcal{B}_{\mathbb{A}\otimes\mathbb{B}}}$). [*Hint: Kronecker product.*]

SOLUTION

We will take the Kronecker product of the two matricies to produce a new matrix:

$$(R \times T)_{\mathcal{B}_{\mathbb{V}\otimes\mathbb{S}} \to \mathcal{B}_{\mathbb{A}\otimes\mathbb{B}}} = (R)_{\mathcal{B}_{\mathbb{V}} \to \mathcal{B}_{\mathbb{A}}} \otimes (T)_{\mathcal{B}_{\mathbb{S}} \to \mathcal{B}_{\mathbb{B}}} = \begin{bmatrix} 2 & -1 & -4 & 2 & 2 & -1 \\ -1 & 2 & 2 & -4 & -1 & 2 \\ -6 & 3 & 4 & -2 & 2 & -1 \\ 3 & -6 & -2 & 4 & -1 & 2 \end{bmatrix}$$