Sedat Akleylek'in cevap vermeden kaçtığı sorularımın son hali, Ercan Çağlar'ın cevaplar.doc dosyasındakilerden biraz farklı ve fazla ve cevapları çok sade !

Hiçbir soruma CEVAP VERMEMİŞ. Doktora tezindeki AKLA ZARAR HATALl lafları tekrar etmiş ve yeni AKLA ZARAR HATALl laflar söylemiş ! AKLA ZARAR OLMAYAN bir tek laf YOK !

Cevaplardaki AKLA ZARAR HATALARdan örnekler :

AKLA ZARAR HATA 1 – EN ÖLÜMCÜL HATA :

Bilgisayarda VERİ YAPILARI diye bir kavram var. Ercan Çağlar, VERİ YAPILARI kavramından HABERSİZ ! Derslerin % 80'i bomboş geçerek bilgisayar mühendisi diploması aldığı için !

Sender, receiver a 1 bit (veya qubit) gönderecek. Göndermeden önce R (Ry) matrisi ile çarpıyor. R (Ry) (içinde sinus ve cosinus var ; yani, veri tipi FLOATING POINT).

Sender, Receiver'a 1 bit (veya qubit) yerine en az 32 veya 64 bit (veya qubit) FLOATING POINT veri tipi gönderiyor ! Yani veriyi acaip bozarak gönderiyor.

Receiver, Sender'ın 1 bit (veya qubit) yerine 32 veya 64 bit (veya qubit) FLOATING POINT gönderdiğini bilmiyor. Bilse de farketmez. Receiver'ın, Sender'ın gönderdiği şifrelenmiş verileri çözme ihtimali SIFIR ! Veriler şifrelenMEmiş olsa da verilerin ne olduğunu anlama ihtimali SIFIR !

Açının kullanılma amacı farklı genliklere sahip süperpozisyon durumunu elde etmektir. Sadece Alice tarafından bilinen farklı değere sahip açılar ile her bir kubite rotasyon kapısı uygulanır. Ve süper pozisyon durumu elde edilir (Denklem 9). Alice, süperpozisyon halindeki kuantum durumu Bob'a gönderir.

AKLA ZARAR HATA 2 :

R(a) x R(-a) matrisi işlemi =DEĞİL Identity matrisi !

"R(a) x R(-a) matrisi işlemi = Identity matrisi" diyor. İşlemi yapıp göstermiyor !

Rotasyon kapısı kullanılan açının negatifi ile süperpozisyon durumuna uygulanırsa başlangıç kuantum durumu elde edilir.

AKLA ZARAR HATA 3 :

Alice ve Bob, birbirini tanımıyor ve şifre anahtarı paylaşmıyor. Ama Bob, Alice'in şifrelemede hangi kapıları kullandığını biliyor. NASIL ? Bob MÜNECCİM mi ?
Yöntem şifreleme ve şifre çözme işlemi için gerekli olan gizli anahtarı paylaşmaz.
Alice ve Bob, yerel olarak gizli anahtarı oluştururlar.
Şekil 2 ve Şekil 3 te görüleceği gibi Alice 2n lik bir klasik veriyi Bob ile paylaşır.
Alice ve Bob, aynı kapılara sahip oldukları için 2n bitlik veriye bu kapıları uygulayarak n bitlik gizli anahtarı yerel olarak oluştururlar. Burada önemli olan Alice ve Bob'un aynı kapı bilgisine sahip olmalarıdır.

AKLA ZARAR HATA 4 :
Veriler Sender ile Receiver arasında ping pong topu gibi gidip geliyormuş. Receiver git-gellerin bittiğini nasıl anlayacak ?? Belli değil. Sonsuz döngüye girer bitmezse ne yapacak ?? Belli değil.
Her kubite ödül değeri veriyormuş ; yani kubitin değerini BOZUYOR ! Kubit zaten 1 çift bit ! Ödül vermeye başladığını Receiver'a nasıl haber veriyor ?? Ve Receiver, Sender'ın hangi kubitlere ödül verdiğini nasıl anlıyor ???
Alice ve Bob'un farklı kapıyı seçtikleri kubitler için Alice başlangıç değerini elde edemez. Bu nedenle o kapının öğrenilmediğini tespit eder. Öğrenilip öğrenilmemesine göre her kubite bir ödül değeri verir ve bunu Bob ile paylaşır. Tüm ödül değeri 1 olana kadar işlemler tekrar eder.Alice ve Bob'un farklı kapıyı seçtikleri kubitler için Alice başlangıç değerini elde edemez. Bu nedenle o kapının öğrenilmediğini tespit eder. Öğrenilip öğrenilmemesine göre her kubite bir ödül değeri verir ve bunu Bob ile paylaşır. Tüm ödül değeri 1 olana kadar işlemler tekrar eder.

Öğrenme eyleminin başarılı olup olmadığına nasıl karar verilir? Alice ve Bob, 3 kapıdan 1 tanesini seçecektir. Bob, Alice'in seçtiği kapıyı bulmaya çalışır. Eğer her ikisi aynı kapıyı seçtiyse tüm işlemlerin sonunda Alice başlangıç değerini elde edecektir. Ödül olarak 1 değeri kabul edilir. Farklı kapıyı seçtikleri durumda Alice başlangıç değerini elde edemez ödül değeri sıfır kabul edilir. Bob, ödül değeri sıfır olan kubitler için ilk seçiminden farklı bir seçim yaparak yeni bir kapı seçer. Bu işlem tüm kapılar öğrenilene kadar devam eder. (S.26)

She sends the reward value to Bob.

Metin güvenlik gerekçesi ile öğrenilemeyen yani 0 ödül değerine sahip kapıların duyurulması ile ilgilidir. Ödül değeri 0 olan kapıların %50'si paylaşılır. Bunun nedeni Eve, Alice kendini Bob, Bob'a ise Alice olarak göstermeye çalışabilir. Eve'yi tespit etmek amaçlı kullanılmaktadır. Eğer Alice ve Bob aynı kapıya sahipse ödül değeri kesinlikle 1 olmalıdır. Bob, Alice'in duyurduğu kapı ile aynı kapıyı seçti ise 1 yerine 0 değerini aldığı için Eve'nin varlığını duyurur.

AKLA ZARAR HATA 5 :
CNOT : 2 bitlik (veya qubitlik) islem, 1 bite (veya qubit) uygulamak MÜMKÜN DEĞİL !
Gate yani kapılar I, X ve CNOT'tan biridir. Bu kapılar gizli anahtarı oluşturmak için kullanılmaktadır. Bob, doğru kapıyı bulduğunu Alice'in ödül değerine göre anlıyor. Peki Alice ödül değerine nasıl karar veriyor? Alice'in CNOT kapısını öğretmek istediğini düşünelim.

n tane kapı öğretilmek için 2n kubitlik kuantum durum kullanılmaktadır. 2 kubitimizin ilk kubitleri kontrol diğeri ise hedef kubittir.
“ qubits are defined as control qubits. qubits are defined as target qubits. Since the control qubit will not be used for the I and X gates, the gates are applied as II and I to the 2-qubit state.” (S.26)
Yukarıdaki metinden anlaşılacağı üzere I ve X kapıları için kontrol kubitine I kapısı uygulanırken, hedef kubite I ya da X kapısı hangisi seçilmişse o uygulanır.

***
***

Ercan Çağlar Cevaplar :

SORU - SIFRELEME SIFRE COZME (kriptoloji) :
Alice (sender) sifreli mesaj gonderiyor , 32 - 64 - 128 veya 195 (??) bit sifreli , sifreleme islemi AÇI da iceriyor (0..360) , ama sifre anahtari gondermiyor. Bob (receiver) sifreyi kendi kendine cozebilir mi ?

CEVAP: 32 64 128 195 bit uzunluğunda gizli anahtarın oluşturulması için gerekli olan kuantum kapı sayısı bit sayısına eşittir. Tablo 2’de belirtilen bu değerler bu boyuttaki anahtarı oluşturacak kapıların öğrenilmesi ile ilgilidir. Açıklama kısmında belirtilmiştir.

“The proposed study performs the learning action with an accuracy of 87.95% for 195 gates, 85.47% for 128 gates, 83.59% for 64 gates, 76.25% for 32 gates. “

Yöntem şifreleme ve şifre çözme işlemi için gerekli olan gizli anahtarı paylaşmaz. Alice ve Bob, yerel olarak gizli anahtarı oluştururlar. Şekil 2 ve Şekil 3 te görüleceği gibi Alice 2n lik bir klasik veriyi Bob ile paylaşır. Alice ve Bob, aynı kapılara sahip oldukları için 2n bitlik veriye bu kapıları uygulayarak n bitlik gizli anahtarı yerel olarak oluştururlar. Burada önemli olan Alice ve Bob’un aynı kapı bilgisine sahip olmalarıdır. Açının kullanılma amacı farklı genliklere sahip süperpozisyon durumunu elde etmektir. Sadece Alice tarafından bilinen farklı değere sahip açılar ile her bir kubite rotasyon kapısı uygulanır. Ve süper pozisyon durumu elde edilir (Denklem 9). Alice, süperpozisyon halindeki kuantum durumu Bob’a gönderir. Bob, bu duruma kendi seçmiş olduğu kapıları uygular (Denklem 10) ve Alice gönderir. Alice, Bob’dan gelen kuantum duruma kendi kapılarını uygular(Denklem 11). Kuantum kapılar terslenebilir olduğu için Bob ve Alice aynı kapıları uyguladıysa Alice’in elinde Denklem 9’daki durum olacaktır. Alice, elindeki açıların negatif açısı ile rotasyon kapısını uygularsa ilk baştaki kuantum duruma sahip olacaktır. Alice ve Bob’un farklı kapıyı seçtikleri kubitler için Alice başlangıç değerini elde edemez. Bu nedenle o kapının öğrenilmediğini tespit eder. Öğrenilip öğrenilmemesine göre

her kubite bir ödül değeri verir ve bunu Bob ile paylaşır. Tüm ödül değeri 1 olana kadar işlemler tekrar eder.

SORU - MATEMATIK :
2 li bir mattrisi , makalede formul (1) deki sinus ve cosinus lu matris ile carpinca sifreleme oluyormus , sonucu ayni matris ile tekrar carpinca sifre cozuluyormus ve ilk matris elde ediliyormus. mumkun mu ?

Öncelikli formül 1 de verilen matris y ekseninde Rotasyon kapısına ait matristir. Bu matris ile şifreleme ya da şifre çözme işlemi yapılmamaktadır. Makalede şifreleme ya da şifre çözme işlemi yaptığına dair bir ibare bulunmamaktadır. Rotasyon kapısı belli bir açı ile bir kubite uygulanarak farklı genliklere sahip süperpozisyon durumu elde edilir. Rotasyon kapısı kullanılan açının negatifi ile süperpozisyon durumuna uygulanırsa başlangıç kuantum durumu elde edilir. Formül 2 ve Formül 3 te görüleceği üzere ile açıları kullanılarak oluşturulan rotasyon kapısının matrisleri birbirinden farklıdır. Formül 4'te süperpozisyon durumunun elde edilmesi, formül 5'te tekrar başlangıç kuantum durumunun elde edilmesi gösterilmektedir.

SORU : Icadim Quantum Reinforcement Learning dedigi sey , bir ogrenme algoritmasi degil ! "odul veriyorum , 1 ekliyorum" diyor , nedeni belli degil , belli olsa da ise yaramaz.

Takviyeli/Pekiştirmeli öğrenmede temel olarak bir ajan vardır. Ajanın gerçekleştirdiği Eyleme göre ödül/ceza verilerek öğrenip öğrenmediği tespit edilir. Birbirini takip eden ve birbirine bağlı bir dizi eyleme göre öğrenme işlemi gerçekleştirilir. Makalemizde referans 1 olarak belirtilen Dong ve diğerleri tarafından yazılan "Quantum Reinforcement Learning" isimli makalede bir öğrenme algoritmasının Markov karar sürecine dayandığını belirtmektedir. Markov karar süreci 5 faktörden oluşmaktadır. Aynı makalenin 20. Sayfasında QRL'nin 3 alt öğe ile tanımlanabileceği belirtilmiştir. Makalemizin 24. sayfasında bulunan aşağıdaki metinden anlaşılacağı üzere çalışmamız Markov Karar Sürecinin 3 öğesi ile temsil edilmiştir.
"In our study, according to MDP, state space S is represented by two qubits. Action space A is represented by gates {Identity (I), NOT (X) and CNOT}, and r is represented by reward function {0,1}. Each choice is independent and does not affect another. Two qubit states are used to learn one gate. Therefore, the 2n-qubit states are used to learn n gates."
Markov Karar Sürecinde bulunan durum geçiş olasılığı ve kriter fonksiyonu bizim çalışmamızda temsil edilmemiştir. Bunun nedeni her bir öğrenme eyleminin birbirinden bağımsız olmasıdır.
"Each gate is taught independently of the others. There are n different learning actions for n gates." (S.24)
Metninden anlaşılacağı üzere n tane kapı öğrenmek için n tane birbirinden bağımsız öğrenme gerçekleşmektedir. Her bir öğrenme bir kapı yani bir eylem içerdiği için durum geçiş olasılığı dikkate alınmamıştır.
Öğrenme eyleminin başarılı olup olmadığına nasıl karar verilir? Alice ve Bob, 3 kapıdan 1 tanesini seçecektir. Bob, Alice'in seçtiği kapıyı bulmaya çalışır. Eğer her ikisi aynı kapıyı seçtiyse tüm işlemlerin sonunda Alice başlangıç değerini elde edecektir. Ödül olarak 1 değeri kabul edilir. Farklı kapıyı seçtikleri durumda Alice başlangıç değerini elde edemez ödül değeri

sıfır kabul edilir. Bob, ödül değeri sıfır olan kubitler için ilk seçiminden farklı bir seçim yaparak yeni bir kapı seçer. Bu işlem tüm kapılar öğrenilene kadar devam eder. (S.26)

SORU: 2021 de tez konusuna TPE den patent aldim , diyor , tez bitmeden 3 yil once , islem suresi 1 yil olsa , 4 yil once.

TR 2021 019962 B patentimiz için, 15.12.2021 tarihinde "Patentle Türkiye 3. Üniversiteler Patent Yarışması" 'na katılarak Patent başvurusunu yaptım. 21.12.2022 tarihinde patent belgesi verildi. 28 Nisan 2023 tarihinde ise yarışmada 7.lik ödülü kazandık.
https://www.turkpatent.gov.tr/haberler/patentle-turkiye-3-universiteler-patent-yarismasi-odul-toreninde-oduller-sahiplerini-buldu

Soru: "Yontemim sifreleme anahtari paylasmiyor , Bob (receiver) sifreyi benim icadim Quantum Reinforcement Learning ile kendi kendine ogreniyor" diyor :

Yöntemimiz şifreleme için kullanılan gizli anahtarı paylaşmıyor. "Instead of sending the secret key, the parties locally generate the required secret keys for each communications." Metninden anlaşılacağı üzere gizli anahtarı paylaşmayıp yerel olarak üretiyor. Şifreyi, QRL ile kendi kendine öğrendiğine dair bir ibare bulunmamaktadır. Bob, QRL ile öğrenmiş olduğu kuantum kapıları kullanarak gizli anahtarı yerel olarak üretmektedir. Şekil 2 ve Şekil 3'te gizli anahtarın nasıl oluşturulduğu görülmektedir. Her iki kullanıcı aynı kuantum kapılara sahiptir. Alice, 2n bitlik bir klasik veri paylaşıyor. Daha sonra her iki kullanıcı, kuantum kapıları kullanarak n bitlik gizli anahtarı yerel olarak üretirler.

SORU: "Bob (receivver) , Alice in (sender) sifreleme islemimi (gate) bulursa odul 1 veriyorum" diyor. Bob , buldugunu nereden biliyor ?????

Öncelikle gate şifreleme işlemi değil. Gate için öyle bir ibare bulunmamaktadır. Gate yani kapılar I, X ve CNOT'tan biridir. Bu kapılar gizli anahtarı oluşturmak için kullanılmaktadır. Bob, doğru kapıyı bulduğunu Alice'in ödül değerine göre anlıyor. Peki Alice ödül değerine nasıl karar veriyor? Alice'in CNOT kapısını öğretmek istediğini düşünelim. Alice'in elinde klasik bir veri var. Bunu 10 olarak kabul edelim. Kuantum durum olarak ifade edersek olacaktır. Bob CNOT kapısını seçtiyse yeni durum olacaktır. Alice kendi kapısı CNOT'ı bu duruma uygularsa başlangıç durum olan 'ı elde eder. Başlangıç değerini elde ettiği için ödül değerini 1 kabul eder. Eğer Bob, I kapısını uygularsa kuantum durum olarak kalacaktır. Alice, CNOT kapısını uyguladığı zaman durumunu elde edecektir. Başlangıç değerinden farklı olduğu için ödül değerini 0 olarak kabul edecektir.
"She compares the 2n bits classical data in Equation (12) with the 2n bit classical data in Equation (8). For bits of the same value, she marks the reward value as "1", and "0" for bits of different value. She sends the reward value to Bob. Then she creates a new quantum state $|\psi\rangle$ and repeats the steps. Bob does not change the gates for qubits with a reward value of "1" for the new quantum state. He changes the gate which applies to

qubits with a reward value of ”0”. He chooses a different gate than the one he chose earlier. This algorithm repeats until all reward values are ”1”.”

Tabi kuantum durum Alice tarafından şeklinde gönderilmemektedir. Rotasyon kapısı uygulanarak süperpozisyon haline getirilip öyle gönderilmektedir. Burada daha basit anlatmak için süperpozisyon uygulamadım. Makalenin 27. Sayfasında bulunan örnek incelenirse daha net anlaşılacaktır. Ayrıca tüm ödül değerleri 1 olduğu zaman kontrol kubitlerinin NOT'ı alınarak tekrar işlem yapılır. Bunun amacı kontrol kubitinin 1 olduğu durumda X ve CNOT kapısı hedef kubite aynı işlemi yapacağı için hataları ayıklamaktır.
“When all reward values are ”1”, the steps are repeated by applying the NOT gate to the control
qubit. If all of the reward values remain as ”1”, error checks are started. Otherwise, iteration continues for bits with a reward value of 0.”

Soru sorulan tarafından aşağıdaki metin paylaşılmıştır.
“In each iteration, Alice announces 50% of the gates which have a reward value of ”0”. Alice and Bob certainly do not choose the same gate when the reward value is ”0”. If they chose the same gate, the reward value would be ”1” with 100% probability.”

Paylaşmış olduğu metin soruyla ilgili değildir. Burada ödül değerinin ne olduğuna karar verilmemektedir. Metin güvenlik gerekçesi ile öğrenilemeyen yani 0 ödül değerine sahip kapıların duyurulması ile ilgilidir. Ödül değeri 0 olan kapıların %50'si paylaşılır. Bunun nedeni Eve, Alice kendini Bob, Bob'a ise Alice olarak göstermeye çalışabilir. Eve'yi tespit etmek amaçlı kullanılmaktadır. Eğer Alice ve Bob aynı kapıya sahipse ödül değeri kesinlikle 1 olmalıdır. Bob, Alice'in duyurduğu kapı ile aynı kapıyı seçti ise 1 yerine 0 değerini aldığı için Eve'nin varlığını duyurur.

Soru: AÇI ???? : (sf 27) Step 2: Alice applies the rotation gate with a different angle for each qubit.
Alice, kuantum durumu süperpozisyon haline getirmek için rotasyon kapısını kullanır. Yani belli bir açıyla y ekseninde döndürerek süperpozisyon durumuna getirir. Ağı dinleyen birisi, süperpozisyon durumunda olduğu için 0 ya da 1'den hangisi olduğunu öğrenemez. Her bir kubit için farklı açı seçilerek farklı genliklere sahip süperpozisyon durumu elde edilir.

SORU: "I, X, CNOT uyguladim" dese de I, X : 1 bitlik islem CNOT : 2 bitlik islem , 1 bite uygulamak mumkun degil ! (sf 24) Alice determines the n gates she will use to generate > the secret key from the {I, X, CNOT} gates.

n tane kapı öğretilmek için 2n kubitlik kuantum durum kullanılmaktadır. 2 kubitimizin ilk kubitleri kontrol diğeri ise hedef kubittir.
“ qubits are defined as control qubits. qubits are defined as target qubits. Since the control qubit will not be used for the I and X gates, the gates are applied as II and I to the 2-qubit state.” (S.26)
Yukarıdaki metinden anlaşılacağı üzere I ve X kapıları için kontrol kubitine I kapısı uygulanırken, hedef kubite I ya da X kapısı hangisi seçilmişse o uygulanır.