

Estudo de caso de Deep Q-Learning

Vítor Kei Taira Tamada

Programa:
Bacharelado em Ciência da Computação

Orientador:
Prof. Dr. Denis Deratani Mauá

São Paulo, novembro de 2018

Estudo de caso de Deep Q-Learning

Esta é a versão original da monografia elaborada pelo
aluno Vítor Kei Taira Tamada

Resumo

TAMADA, V. K. T. **Estudo de caso de Deep Q-Learning**. Trabalho de Conclusão de Curso - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2018.

Visualização de imagem, abstração de informação e aprendizado por recompensa são tarefas que seres humanos aprendem consideravelmente rápido. Computadores, por outro lado, podem levar horas ou até dias para aprender algo que pessoas fariam em segundos, principalmente quando envolve interpretação de imagens.

Este trabalho buscou estudar a eficiência e capacidade de um agente aprender utilizando *deep Q-learning*. Aplicando a técnica em três ambientes de características e complexidade diferentes, *Gridworld*, *Pong* e *Asteroids*, foi analisado o grau de sucesso ou insucesso que a inteligência artificial teve neles. No fim, ao observar resultados correspondentes ao nível de dificuldade de cada domínio, é feita uma discussão sobre como suas diferenças foram relevantes para esses níveis de aprendizado.

Palavras-chave: inteligência artificial, deep q-learning, estudo de caso

Sumário

1	Introdução	1
1.1	Motivação e Proposta	1
1.2	Ferramentas	2
1.2.1	<i>Gridworld</i>	2
1.2.2	<i>Pong</i> - Atari2600	2
1.2.3	<i>Asteroids</i> - Atari2600	3
1.2.4	Gym & Gym-Retro	3
1.2.5	TensorFlow	4
1.3	Proposta	4
2	Fundamentos	5
2.1	Redes neurais	5
2.2	Aprendizado profundo	7
2.3	Rede neural convolucional	7
2.4	Processo de Decisão de Markov	8
2.5	Aprendizado por reforço	9
2.6	<i>Q-learning</i>	10
2.7	<i>Approximate Q-learning</i>	11
2.8	<i>Deep Q-Learning</i>	12
2.9	Aprimorando o aprendizado	13
2.9.1	<i>Experience Replay</i>	13
2.9.2	Alvo fixo	13
3	Implementação	15
3.1	Arquitetura	16
3.1.1	<i>Gridworld</i>	16
3.1.2	<i>Pong</i>	16
3.1.3	<i>Asteroids</i>	17
3.2	Experimentos	18
3.2.1	<i>Gridworld</i>	18
3.2.2	<i>Pong</i>	18
3.2.3	<i>Asteroids</i>	18
4	Resultados	19
4.1	<i>Gridworld</i>	19
4.2	<i>Pong</i>	19
4.3	<i>Asteroids</i>	20
5	Conclusão	21
	Referências Bibliográficas	23

Capítulo 1

Introdução

Inteligência artificial, ou IA, é uma área de estudos que pode ser definida de diversas formas, como construir uma máquina que realize com sucesso tarefas tradicionalmente feitas por humanos, ou que aja como um humano. Envolvendo filosofia, matemática, economia, neurociência, psicologia, computação e até mesmo linguística ao longo de sua história, ela abrangeu e ainda abrange diversos campos da ciência, com profissionais de várias formações diferentes podendo contribuir para seus avanços. Existem inúmeros desafios atualmente: alguns resolvidos, como vencer de jogadores profissionais de Xadrez, mas muitos ainda sendo abordados, podendo ser uma busca por alguma solução, ou por uma solução mais eficiente que a já existente.

É interessante a forma como, em particular, seres humanos aprendem. Crianças pequenas e bebês principalmente aprendem interagindo com o ambiente: tocam nos objetos, tentam entender aquilo que os rodeia e qual o resultado de suas ações, mesmo que inconscientemente. Avanços recentes em inteligência artificial permitiram que máquinas simulem esse tipo de aprendizado por meio de **aprendizado por reforço**. Entretanto, para muitos casos, só essa técnica não é o suficiente. Utilizando jogos como exemplo, uma pessoa consegue inferir o que é inimigo e o que é terreno quando aparece na tela do jogo em poucos movimentos ou até já supor a partir de experiências passadas com jogos diferentes. Para um computador, um pixel que mude de posição já faz ele não conseguir mais distinguir o que está vendo, tendo que reaprender a cada nova combinação de pixels detectada. Em outras palavras, seres humanos conseguem abstrair as informações que enxergam com facilidade, enquanto os computadores não.

Se computadores não conseguem mais identificar um objeto na tela por causa de um pixel que esteja diferente, como sistemas de detecção de imagem funcionam? Utilizando uma variante de rede neural profunda (*deep neural network*) chamada **rede neural convolucional** (*convolutional neural network* (CNN)), é possível fazer uma inteligência artificial abstrair essas informações e inferir que um objeto em diferentes lugares da tela, assumindo diferentes tamanhos, são o mesmo.

1.1 Motivação e Proposta

A proposta deste trabalho surgiu do interesse por uma técnica de aprendizado de máquina não estudada nas disciplinas de inteligência artificial do curso. Aplicando os conhecimentos adquiridos na faculdade, o objetivo deste trabalho é fazer um estudo de caso de *deep Q-learning* aplicado a ambientes com características distintas.

As ferramentas utilizadas, descritas na próxima seção, foram o Gym e Gym-Retro como interface, o Stella como emulador e a API do TensorFlow para a computação. As técnicas de aprendizado de máquina aplicadas, descritas no capítulo seguinte, foram **aprendizado por reforço** e **rede neural**

convolucional, mais especificamente a união das duas, conhecida como *deep reinforcement learning* ou *deep Q-learning* [Mni+13].

Espera-se conseguir construir arquiteturas de *deep Q-learning* pela qual o agente consiga montar um modelo que tenha sucesso no respectivo ambiente.

1.2 Ferramentas

Nesta seção, serão apresentados os ambientes e as principais ferramentas utilizadas no desenvolvimento deste trabalho, uma breve descrição sobre elas e o motivo de suas escolhas.

1.2.1 Gridworld

Gridworld é um exemplo clássico em estudos e ensinamentos de aprendizado por reforço. Ele consiste em um mapa de espaços quadrados em que o agente começa em um deles e pode se mover para cima, direita, esquerda ou baixo, contanto que o espaço seja válido. Alguns dos espaços geram recompensa positiva (objetivo) e outros geram recompensa negativa (armadilha) ao ser alcançado, além de encerrarem o episódio e fazerem o agente retornar ao ponto inicial. O desenvolvedor pode optar por gerar pequenas recompensas positivas ou negativas a cada passo, mesmo que não alcance um estado terminal, para analisar seu comportamento em tais circunstâncias.

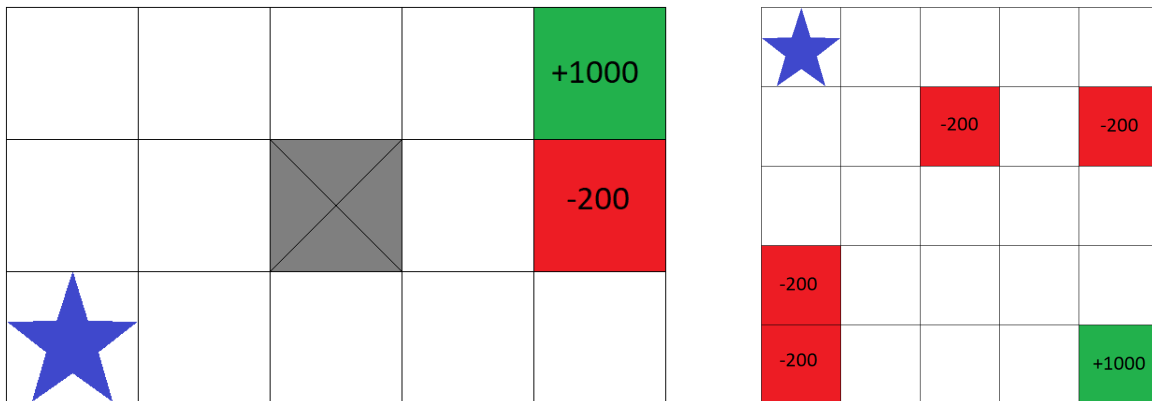


Figura 1.1: Exemplos de mapas de *Gridworld*. A estrela azul indica a posição inicial do agente, o espaço cinza com um \times indica um espaço inválido, o verde com +1000 representa o objetivo e os vermelhos com -200 representam as armadilhas.

O número de estados deste ambiente é igual ao número de espaços válidos, uma vez que são definidos pela posição em que o agente se encontra.

Gridworld é o ambiente mais simples estudado neste trabalho.

1.2.2 Pong - Atari2600

Pong foi um dos primeiros jogos criados e o primeiro desenvolvido pela Atari, lançado em novembro de 1972. O jogo simula uma partida de tênis de mesa por meio de duas barras verticais, uma do lado esquerdo e uma do lado direito, e uma bola que se move pela tela. Cada jogador controla uma das barras movendo-a para cima e para baixo, rebatendo a bola para evitar que chegue no fim da tela do próprio lado enquanto tenta fazê-la chegar no fim da tela do lado do adversário. A principal diferença entre as versões do jogo é o número de pontos necessários para vencer.

A versão do *Pong* utilizada neste trabalho é a do Atari2600, emulada pelo emulador Stella. Nesta iteração, vence o jogador que fizer 21 pontos primeiro.

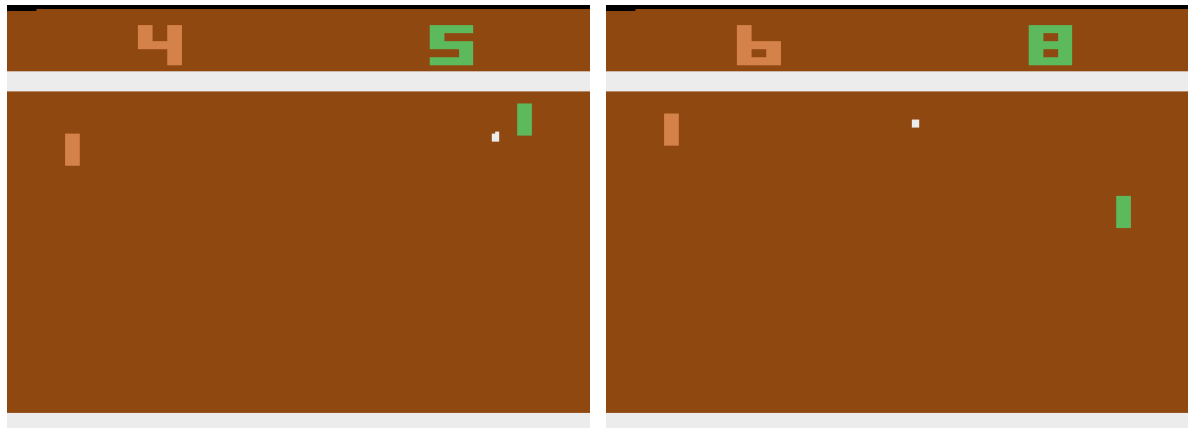


Figura 1.2: Exemplos de tela do jogo no emulador Stella. O jogador controla a barra verde, do lado direito da tela caso o oponente seja a IA escrita pelos desenvolvedores. O ponto branco no meio da tela é a bola, as barras brancas representam os limites superior e inferior do campo e os números no topo indicam a pontuação de cada jogador.

Os estados são definidos pela tela do jogo, que é uma matriz de 210x160 pixels, com cada pixel tendo 3 canais de cor. Esses canais variam de 0 a 255 e a combinação de seus valores determinam a cor do pixel dentro de uma paleta de 128 cores.

Pong é o ambiente de complexidade média estudada neste trabalho.

1.2.3 Asteroids - Atari2600

Asteroids é um jogo de fliperama lançado em novembro de 1979 pela Atari. O jogador controla uma nave espacial em um campo de asteróides, tentando destruí-los enquanto tenta sobreviver. Quando um asteróide é destruído, outros menores aparecem no lugar. As principais diferenças entre as iterações de *Asteroids* incluem a presença de naves espaciais inimigas que atiram contra o jogador, formatos e tamanhos diferentes dos asteróides e direção que eles se movem.

A versão de *Asteroids* utilizada neste trabalho é a do Atari2600, emulada pelo emulador Stella. Nesta iteração, não existem naves espaciais inimigas, apenas asteróides que assumem três tamanhos distintos, começando sempre pelo maior, que vale menos pontos enquanto o menor vale mais. A principal forma de destruir um asteróide e ganhar pontos é atirando neles. O jogador possui quatro vidas inicialmente e cinco ações para jogar: mover-se para frente, girar a nave no sentido horário, girar a nave no sentido anti-horário, mover-se no hiper-espaco, e atirar para frente. Mover-se para frente e girar são as principais formas de movimento no jogo, enquanto atirar é a de destruir asteróides e ganhar pontos. Mover-se no hiper-espaco consiste em fazer a nave desaparecer por alguns instantes e reaparecer em um local aleatório da tela.

Assim como no *Pong*, os estados são compostos por uma matriz de 210x160 pixels, cada um tendo 3 canais que determinam a cor.

Asteroids é o mais complexo dos ambientes estudados neste trabalho.

1.2.4 Gym & Gym-Retro

Gym é uma plataforma para pesquisa de aprendizado por reforço desenvolvida e mantida pela empresa de pesquisas em inteligência artificial OpenAI. Esta ferramenta auxilia na emulação de diversos ambientes diferentes, incluindo alguns poucos jogos de Atari (*Pong* incluso, mas *Asteroids* não) e ambientes 3D. Utilizou-se o *Frozen Lake*, removendo a aleatoriedade dos movimentos e criando um mapa personalizado do tamanho desejado, e o *Pong* do Gym neste trabalho.

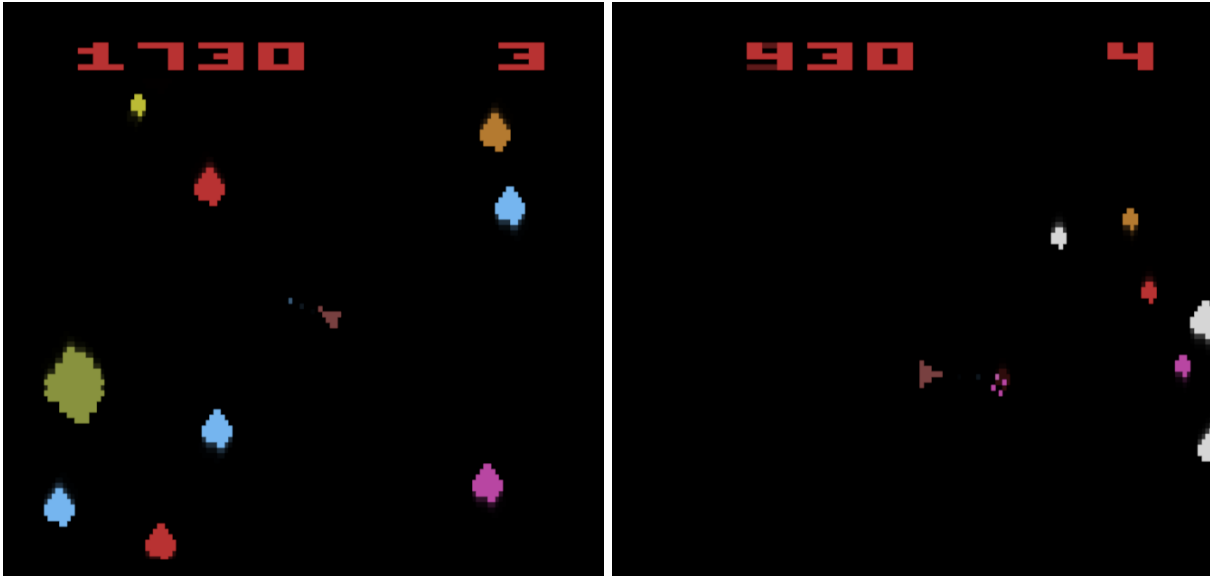


Figura 1.3: Exemplos de tela do jogo no emulador Stella. O número no canto superior esquerdo é a pontuação e o do canto superior direito é a quantidade de vida restante que o jogador tem. A nave é o triângulo no meio da tela, o ponto azul próximo dela na imagem da esquerda é um tiro e o restante é asteróide. Na tela da direita, um asteróide acaba de ser destruído.

Gym-Retro é uma variante da Gym com ênfase em jogos eletrônicos antigos, como dos consoles Sega Genesis, Nintendo Entertainment System e Atari2600. Para qualquer jogo que o usuário deseje emular, é necessário que ele tenha a ROM (*Read Only Memory*) do jogo. Utilizou-se o *Asteroids* do Gym-Retro neste trabalho.

O principal motivo de estas ferramentas terem sido escolhidas é por permitirem emular o *Pong* e o *Asteroids*, além de possuir um ambiente semelhante ao *Gridworld*.

1.2.5 TensorFlow

TensorFlow é um arcabouço de código aberto para computações numéricas de alta performance, desenvolvido e mantido pela Google. Seu núcleo de computação numérica flexível permite o uso da biblioteca em diversos campos científicos. Oferece, em particular, grande suporte a aprendizado de máquina e aprendizado profundo, ou, como é mais conhecido, *deep learning*. Esta ferramenta foi escolhida por oferecer uma API em Python estável, ter grande suporte, comunidade ativa, e ser de código aberto.

1.3 Proposta

A proposta deste trabalho é fazer um estudo de caso da técnica *deep Q-learning* em três ambientes digitais diferentes e ver o grau de sucesso obtido em cada um, utilizando como entrada apenas a tela do jogo (considerando o mapa do *Gridworld* com o agente inserido como uma tela). Gym e Gym-Retro servirão de interface enquanto o Stella emulará o jogo. As técnicas de aprendizado de máquina utilizadas serão **aprendizado por reforço** e **rede neural convolucional**, em particular o *deep Q-learning*, que é a junção dessas duas.

Capítulo 2

Fundamentos

Para se criar e treinar uma inteligência artificial, diversos arcabouços são necessários. Por um lado, existe a parte teórica e matemática na qual a inteligência se baseia para aprender. Por outro, do lado computacional, existem as bibliotecas que auxiliam no desenvolvimento, efetuando as contas necessárias e, neste trabalho em particular, emulando o jogo que serve de ambiente para o aprendizado. Este capítulo tem o intuito de familiarizar o leitor com a teoria e fundamentos técnicos utilizados na modelagem e treinamento da inteligência artificial deste trabalho.

2.1 Redes neurais

Redes neurais artificiais, mais conhecidas como redes neurais, são uma forma de processamento de informação inspirada no funcionamento do cérebro. Assim como o órgão no qual foi baseada, elas possuem uma grande quantidade de elementos de processamento de informação conectados entre si chamados de neurônios, que trabalham em conjunto para resolver problemas. Dado que aprendem com exemplos, similar a pessoas, é considerada uma técnica de aprendizado supervisionado.

Com os avanços nos estudos dessa técnica nos últimos anos, diversos tipos diferentes de redes neurais foram desenvolvidos, como redes neurais convolucionais (*Convolutional Neural Networks*, CNN), a utilizada neste trabalho, e redes neurais de memória de curto-longo prazo¹ (*Long/Short Term Memory*, LSTM), que não será abordada. Apesar de cada uma ter sua particularidade, redes neurais clássicas possuem duas características principais: os **neurônios**, e a estrutura dividida em **camadas**. Existem redes que não são consideradas clássicas pela falta de estrutura em camadas, como Redes de Hopfield (*Hopfield Network*) e Máquinas de Boltzmann (*Boltzmann Machine*), que não serão discutidas neste trabalho.

Neurônios são funções que recebem como entrada a saída de cada neurônio da camada anterior e devolvem um número, em geral entre 0 e 1 inclusive, cujo significado e como são usados variam de acordo com o trabalho em questão.

A estrutura de uma rede neural clássica é dividida em **camadas** que podem ser classificadas de três formas distintas: **entrada**, **oculta**, ou **saída**. A de **entrada** é a que a IA usa para receber os dados que serão processados; as camadas **ocultas** (*hidden layers*) são o processamento; e a de **saída** devolve uma série de números utilizados pela IA para tomar uma decisão ou fazer uma predição. Pode-se dizer que uma rede neural é um aproximador de uma função que mapeia entrada e saída. Enquanto o número de neurônios na entrada e na saída são definidos pelo trabalho em questão, o de camadas ocultas e de neurônios em cada uma delas são arbitrários, sendo normalmente definidos por meio de tentativa e erro.

Cada neurônio das camadas ocultas representa uma característica (*feature*) detectada ao longo do

¹Tradução livre feita pelo autor

treinamento. Se essa característica estiver presente na camada de entrada, então o neurônio correspondente será **ativado**. A ativação de um ou mais neurônios pode levar a ativação de outros neurônios na camada seguinte e assim sucessivamente. Esse é um comportamento inspirado na forma como neurônios do cérebro enviam sinais de um para o outro. Em redes neurais artificiais, um neurônio é ativado quando a soma dos números de entrada passa de um certo valor e por uma função de ativação.

Porém, nem todos os valores de entrada devem ser igualmente importantes, então cada um desses números recebe um peso que determina sua importância para a ativação da característica. Matematicamente, isso é representado da seguinte forma: seja n o número de neurônios na camada anterior, w_i , $i = 1, \dots, n$, os pesos das saídas de cada neurônio da camada anterior, e a_i , $i = 1, \dots, n$, o valor de saída de cada neurônio da camada anterior e, por consequência, cada valor de entrada do neurônio atual, e b o viés (*bias*) da função.

$$w_1a_1 + w_2a_2 + \dots + w_na_n - b \quad (2.1)$$

Como essa soma pode ter qualquer valor no intervalo $(-\infty, +\infty)$, o neurônio precisa saber a partir de que ponto ele estará ativado. Para isso, utiliza-se uma **função de ativação**. Funções de ativação recebem a soma 2.1 como entrada, limitam seu valor a um certo intervalo e determinam se o neurônio deve ser ativado ou não.

Esse procedimento é feito em cada neurônio de cada camada da rede neural, o que pode ser muito custoso se não executado com cuidado. Como existem diversas bibliotecas que otimizam operações matriciais, é mais rápido e conveniente utilizar matrizes, além de facilitar a leitura do código: seja W a matriz tal que cada linha contém os pesos de cada neurônio da camada anterior para um determinado neurônio da camada atual, $a^{(i)}$ o vetor tal que cada elemento é o valor de saída de cada neurônio da camada anterior, e b o viés, é possível efetuar a soma 2.1 para todos os neurônios de uma camada da seguinte forma:

$$Wa^{(i)} + b, \quad i = 1, \dots, n \quad (2.2)$$

As funções de ativação mais comuns são a sigmoide (curva logística), ReLU (*Rectified Linear Unit*) e ELU (*Exponential Linear Unit*), sendo a sigmoide a mais antiga e a ELU a mais recente.

O próximo passo é entender como os valores dos neurônios e os respectivos pesos são utilizados para a inteligência conseguir soltar a resposta correta. Como mencionado anteriormente, conforme as características se mostram presentes na camada de entrada, os neurônios referentes a esses atributos são ativados até que o neurônio com a resposta dada pela inteligência artificial seja ativado. Como rede neural é um tipo de aprendizado supervisionado, os exemplos inseridos nela possuem rótulos, saídas esperadas (qual valor que cada neurônio de saída deve ter). Para que o computador saiba o quão ruim foi sua saída, é definida uma função de erro, também conhecida como função de custo. Em muitos casos, utiliza-se o erro quadrático médio, que dá mais peso para erros maiores uma vez que a diferença é elevada ao quadrado, mas existem diversas funções diferentes para isso. Naturalmente, quanto maior for o erro, mais incorreta foi a previsão. Depois de esse procedimento ser feito com milhares ou até milhões de exemplos, calcula-se a média dos erros obtidos e, com isso, avalia-se o desempenho da inteligência.

Otimizar os pesos de forma que se reduza a média dos erros obtidos com os exemplos parece ser o melhor caminho para melhorar o modelo, mas isso não é necessariamente verdade. Os milhares de exemplos utilizados nessa etapa compõe o conjunto de treinamento. Se o modelo tiver erro zero em relação a esse conjunto, ele estará sofrendo de *overfitting*: a inteligência se adequa tanto ao conjunto de treinamento que saberá o que fazer apenas nele. O mais desejável é minimizar o erro sobre todos os dados possíveis ou, no mínimo, os esperados em cenários reais, e o conjunto de treinamento dificilmente

conseguirá abranger todos eles.

De forma resumida, uma rede neural clássica aprende recebendo uma série de números como entrada e devolve uma saída; calcula-se o quão errada essa saída está em relação ao desejado para aquela determinada entrada, e ajusta os pesos conforme a necessidade para minimizar o erro; após repetir esses passos milhares de vezes, espera-se que a IA tenha aprendido o suficiente a resolver o problema em mãos.

2.2 Aprendizado profundo

Como explicado anteriormente, redes neurais podem ser divididas em três tipos distintos de camadas: entrada, ocultas, e saída. Enquanto existe apenas uma camada de entrada e uma de saída, é possível haver uma ou mais camadas ocultas. Se houver muitas camadas ocultas, a rede neural passa a ser chamada de rede neural profunda (*deep neural network*). Atualmente, não existe uma definição exata de quantas camadas a rede neural precisa ter para começar a ser classificada como profunda e, mesmo que houvesse, esse número provavelmente mudaria com o passar do tempo.

Uma rede neural profunda que segue o modelo apresentado na seção anterior é chamada de *feedforward* e é o mais típico de *deep learning*. Ele recebe esse nome pois a informação flui da entrada para a saída sem haver conexões de *feedback* para que a previsão seja feita. Este tipo de rede neural forma a base para **redes neurais convolucionais**, técnica muito utilizada em reconhecimento de imagens. Como a ideia é treinar uma inteligência artificial que aprende vendo imagens do ambiente, esse foi o tipo escolhido para este trabalho.

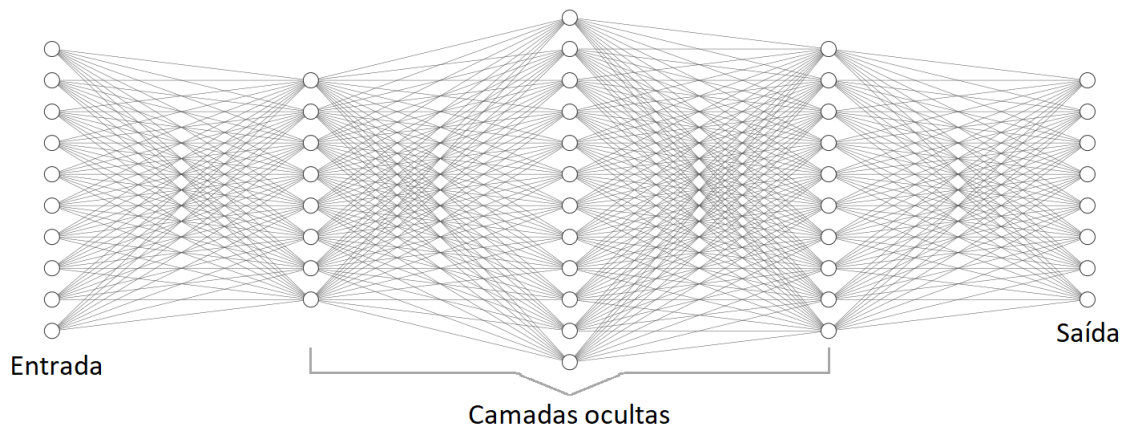


Figura 2.1: Esquema de uma rede neural profunda do tipo *feedforward*. Número de nós e camadas arbitrários para melhor representação. Diagrama feito em <http://alexlenail.me/NN-SVG/index.html>

2.3 Rede neural convolucional

Como neste trabalho a IA precisa aprender características do ambiente apenas enxergando imagens dele, utilizar apenas redes neurais profundas sofre de um problema: o computador não consegue reconhecer um mesmo objeto em diferentes locais da tela e de diferentes tamanhos como o mesmo. Para cada local muito diferente que ele aparecer, como direita e esquerda da tela, a IA teria que re-aprender a identificá-lo.

Para não precisar fornecer à rede neural imagens inteiras para que ela aprenda que um objeto continua sendo o mesmo não importa onde da tela apareça, foi utilizada convolução, mais precisamente a 2D, já que a entrada é uma imagem, uma matriz de pixels. Uma CNN continua sendo um tipo de rede neural profunda e, portanto, mantém o formato de três tipos de camadas (entrada, ocultas, e saída). Porém,

para facilitar o entendimento de convolução, esta explicação dividirá a rede em duas partes: **convolução** e **previsão**. Na etapa de **convolução**, a imagem de entrada é dividida em várias imagens menores; elas podem ser adjacentes ou parcialmente sobrepostas, sendo o segundo caso mais comum. Cada uma dessas imagens menores é chamada de **filtro convolucional**. É possível dizer que se um filtro convolucional for arrastado para o lado, o local onde ele parar será o próximo filtro convolucional, pois o padrão de pixels deverá ser diferente e, portanto, apresentará uma característica diferente que pode ser detectada. Esse arrasto é chamado de passo (*stride*) e a distância que o filtro é arrastado é chamada de tamanho do passo. Em seguida, cada uma dessas imagens menores é passada por uma rede neural menor, sendo processada normalmente. As saídas dessas redes neurais menores são então passadas como entrada para a próxima etapa. Na etapa de **previsão**, a informação passa por uma ou mais redes neurais maiores que farão a previsão. Para diferenciá-la das redes da etapa de convolução, as desta fase são chamadas de *fully-connected*.

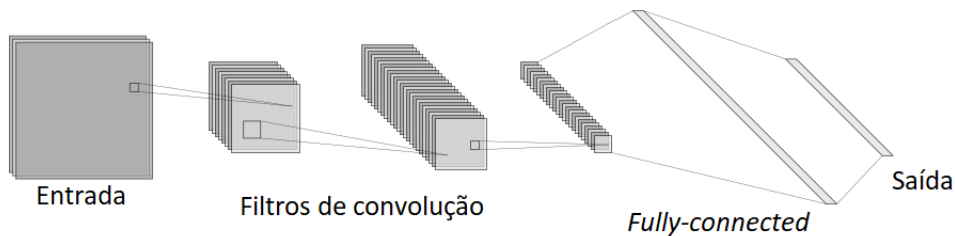


Figura 2.2: Esquema de uma rede neural convolucional. Número de filtros e camadas arbitrários para melhor representação. Diagrama feito em <http://alexlenail.me/NN-SVG/LeNet.html>

É possível haver mais de uma camada de convolução assim como pode haver mais de uma camada *fully-connected*, e isso pode ser mais vantajoso. Quanto mais camadas houver, mais precisa será a predição. Entretanto, não só o custo de tempo e de espaço aumenta, como há um limite para o quão melhor será o desempenho da IA. A partir de um certo ponto, a melhora se torna ínfima em comparação com o tempo despendido e, portanto, deixa de ser benéfico colocar mais camadas.

2.4 Processo de Decisão de Markov

Antes de falar sobre aprendizado por reforço, é necessário explicar o que é um **Processo de Decisão de Markov** (*Markov Decision Process* - MDP). Um MDP padrão possui as seguintes propriedades: a probabilidade de se chegar em um estado futuro S' dado que a inteligência artificial, também conhecida como agente, se encontra no estado S depende apenas da ação A tomada nesse estado S , o que caracteriza a **propriedade Markoviana**; existe um modelo probabilístico que caracteriza essa transição, dado por $P(S'|S, A)$; todos os estados do ambiente e todas as ações que o agente pode tomar em cada estado são conhecidas; e a recompensa é imediatamente recebida após cada ação ser tomada.

As probabilidades de o agente tomar cada ação em um dado espaço são definidas por uma política π . A qualidade de uma política é medida por sua **utilidade esperada**, e a política ótima é denotada por π^* . Para calcular π^* , utiliza-se um algoritmo de iteração de valor que computa a utilidade esperada do estado atual: começando a partir de um estado arbitrário S , tal que seu valor esperado é $V(S)$, aplica-se a equação de Bellman até haver convergência de $V(S)$, que será denotado por $V^*(S)$. Esse $V^*(S)$ é usado para calcular a política ótima $\pi^*(s)$.

Seja i a iteração atual, S o estado atual, S' o estado futuro, A a ação tomada no estado atual, $R(S, A, S')$ a recompensa pela transição do estado S para o estado S' por tomar a ação A , e γ o valor de

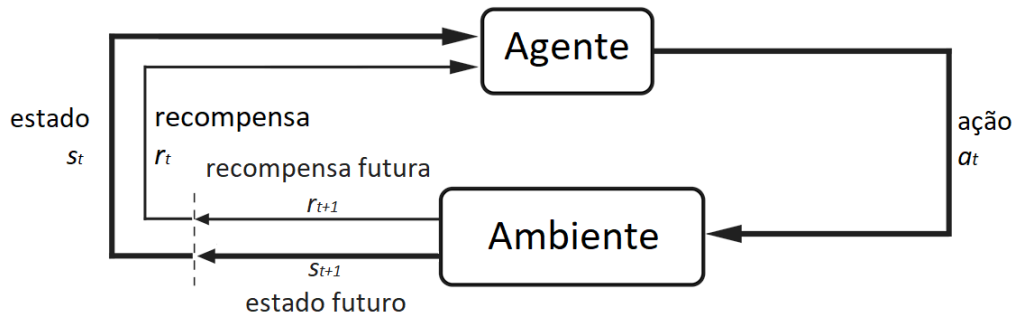


Figura 2.3: Interação agente-ambiente em um processo de decisão de Markov[SB18]. Adaptação e tradução da imagem original feitas pelo autor.

desconto (valor entre 0 e 1 que determina a importância de recompensas futuras para o agente), temos que:

Equação de Bellman:

$$V^{(i)}(S) = \max_A \sum_{S'} P(S'|S, A) [R(S, A, S') + \gamma V^{(i-1)}(S')] \quad (2.3)$$

$$\lim_{i \rightarrow \infty} V^{(i)}(S) = V^*(S) \quad (2.4)$$

Política gulosa para função valor ótima:

$$\pi^*(s) = \operatorname{argmax}_A \sum_{S'} P(S'|S, A) [R(S, A, S') + \gamma V^*(S')] \quad (2.5)$$

Um dado das fórmulas acima comum de se faltar é a probabilidade de transição $P(S'|S, A)$. Portanto, utiliza-se **aprendizado por reforço** para contornar esse problema.

2.5 Aprendizado por reforço

Aprendizado por reforço, diferente do supervisionado e de redes neurais por consequência, não recebe exemplos rotulados para saber o quão correta ou incorreta sua resposta está para cada entrada. Ao invés disso, o agente interage com o ambiente e recebe recompensas positivas, negativas ou nulas por suas ações. Seu objetivo é explorar o espaço de estados a fim de aprender a recompensa esperada para cada ação tomada em cada um deles. Dessa forma, ele saberá o que fazer em cada situação do ambiente em que se encontra.

As recompensas esperadas de cada ação em cada estado são armazenadas em uma tabela que deve mapear todas as ações para todos os estados. Isso é possível em domínios simples, como um Jogo da Velha, mas se torna impraticável conforme o espaço de estados aumenta. No caso do *Pong* e do *Asteroids*, os *frames* do jogo são os estados. Um pixel que mude de cor já faz ser um estado completamente diferente do ponto de vista do computador. Em uma tela de 210x160 pixels, com cada pixel armazenando três números que vão de 0 à 255 para determinar sua cor, é evidente não ser possível armazenar na memória um mapeamento das ações para cada um desses estados. Mesmo que não houvesse esse obstáculo computacional, há muitas situações em que não é possível determinar qual ação retornará a maior recompensa.

Como dito no final da seção [anterior](#), aprendizado por reforço é um MDP que não utiliza as probabilidades de transição para aproximar a política ótima. No contexto deste trabalho, a política ótima será encontrada utilizando uma variante da técnica **Q-Learning**.

2.6 *Q-learning*

Quando não se conhece as probabilidades de transição, informação necessária para se obter a função valor pela equação de Bellman, é possível estimar $V(S)$ a partir de observações feitas sobre o ambiente. Logo, o problema deixa de ser tentar encontrar P e passa a ser como extrair a política do agente de uma função valor estimada.

Seja $Q^*(S, A)$ a função Q-valor² que expressa a recompensa esperada de se começar no estado S , tomar a ação A e continuar de maneira ótima. $Q^*(S, A)$ é uma parte da política gulosa para função valor ótima e é dada por:

$$\begin{aligned} Q^*(S, A) &= \sum_{S'} P(S'|S, A)[R(S, A, S') + \gamma V^*(S')] \\ &= \sum_{S'} P(S'|S, A)[R(S, A, S') + \gamma \max_{A'} Q^*(S', A')] \end{aligned} \quad (2.6)$$

Logo, substituindo 2.6 em 2.5, temos que a política gulosa ótima para a função Q-valor ótima é dada por:

$$\pi^*(S) = \operatorname{argmax}_A Q^*(S, A) \quad (2.7)$$

O próximo passo será entender como atualizar a função Q-valor.

Supondo que o agente se encontra no estado S e toma a ação A , que causa uma transição no ambiente para o estado S' e gera uma recompensa $R(S, A, S')$, como computar $Q^{(i+1)}(S, A)$ baseado em $Q^{(i)}(S, A)$ e em $R(S, A, S')$, sendo i o momento atual? Para responder a essa pergunta, duas restrições precisam ser feitas: $Q^{(i+1)}(S, A)$ deve obedecer, pelo menos de forma aproximada, a equação de Bellman, e não deve ser muito diferente de $Q^{(i)}(S, A)$, dado que são médias de recompensas. A seguinte equação responde a essa questão.

Seja α a taxa de aprendizado (valor entre 0 e 1 que determina o quão importantes informações novas são em relação ao conhecimento que o agente possui),

$$\begin{aligned} Q^{(i+1)}(S, A) &= (1 - \alpha)Q^{(i)}(S, A) + \alpha[R(S, A, S') + \gamma \max_{A'} Q^{(i)}(S', A')] \\ &= Q^{(i)}(S, A) + \alpha[R(S, A, S') + \gamma \max_{A'} Q^{(i)}(S', A') - Q^{(i)}(S, A)] \end{aligned} \quad (2.8)$$

A convergência de $Q^{(i)}(S, A)$ em $Q^*(S, A)$ é garantida mesmo que o agente aja de forma subótima contanto que o ambiente seja um MDP, a taxa de aprendizado seja manipulada corretamente, e se a exploração não ignorar alguns estados e ações por completo - ou seja, raramente. Mesmo que as condições sejam satisfeitas, a convergência provavelmente será demasiadamente lenta. Entretanto, é interessante analisar os problemas levantados pela segunda e pela terceira condição que garantem a convergência e maneiras de solucioná-los.

Se a **taxa de aprendizado** for muito alta (próxima de 1), a atualização do aprendizado se torna instável. Por outro lado, se for muito baixa (próxima de 0), a convergência se torna lenta. Uma solução possível para essa questão é utilizar valores que mudam de acordo com o estado: utilizar valores mais baixos em estados que já foram visitados muitas vezes, pois o agente já terá uma boa noção da qualidade de cada ação possível, então há pouco que aprender; e utilizar valores mais altos em estados que foram visitados poucas vezes, pois o agente precisa aprender melhor sobre ele.

Uma vez que a política é gulosa em relação ao Q-valor, o agente sempre tomará a ação que retorna a maior recompensa esperada. Ou seja, a ação escolhida depende do valor da taxa de desconto γ : re-

²O nome "Q-valor" vem do valor da qualidade da ação

compensas imediatas serão mais buscadas se for próximo de 0, enquanto recompensas futuras serão mais valorizadas para valores próximos de 1. Isso é bom somente se todas as recompensas possíveis para aquele estados são conhecidas. Porém, se houver ações não exploradas, o agente pode perder uma recompensa maior do que as que ele já conhece apenas porque ignorou a ação que leva a ela. Essa situação caracteriza o dilema **Exploration versus Exploitation**: é melhor tomar a ação que retorna a maior recompensa ou buscar uma melhor? Da mesma forma que na taxa de aprendizado, uma forma de contornar esse problema é mudar a probabilidade de decidir explorar o ambiente (*explore*) de acordo com a situação. Conforme o mundo é descoberto, se torna cada vez mais interessante agir de forma gulosa (*exploit*) do que explorar em estados muito visitado, e vice-versa em estados pouco visitados. Esse comportamento pode ser definido por uma função de exploração.

Seja P_{ini} a probabilidade inicial e P_{min} a probabilidade mínima de o agente decidir explorar (*explore*) o ambiente, $decay$ a taxa de decaimento e $step$ o número de passos dados até o momento. A probabilidade de o agente explorar (*explore*) o ambiente é dada por:

$$P_{explore} = P_{min} + (P_{ini} - P_{min})e^{-step/decay} \quad (2.9)$$

Outro problema enfrentado por *Q-learning* é o de generalização. A política $\pi^*(S)$ determina a melhor ação a se tomar em cada estado. Logo, utiliza-se uma tabela para armazenar todas essas escolhas. Porém, como mencionado anteriormente, isso se torna inviável para espaços de estado muito grandes. Portanto, se não é possível aprender os Q-valores, o melhor que se pode fazer é tentar achar uma aproximação deles.

2.7 Approximate Q-learning

Approximate Q-Learning é o nome dado a um conjunto de métodos de aprendizado por reforço que busca aproximar o Q-valor das ações. Uma técnica comum desse conjunto é o uso de **funções lineares** que avaliam características dos estados.

Para lidar com o enorme espaço de estados que alguns ambientes possuem, o agente armazena e aprende apenas algumas propriedades, que são funções de valor real, para tomar as decisões. Tais informações são armazenadas em um vetor e cada elemento desse vetor recebe um peso que determina a respectiva importância para que escolhas sejam feitas. Ou seja, a função Q-valor é representada por uma combinação linear das propriedades e é dada da seguinte forma:

$$Q(S, A) = \omega_1 f_1(S, A) + \omega_2 f_2(S, A) + \dots + \omega_n f_n(S, A) \quad (2.10)$$

Como o $V(S')$ é o valor esperado e $Q(S, A)$ é o valor previsto, a atualização pode ser interpretada como ajustar o Q-valor pela diferença desses dois números. Além disso, como o *approximate Q-learning* avalia características, apenas os pesos precisam ser atualizados:

$$\omega_k^{(i+1)}(S, A) = \omega_k^{(i)}(S, A) + \alpha[R(S, A, S') + \gamma V(S') - Q^{(i)}(S, A)]f_k(S, A), k = 1, 2, \dots, n \quad (2.11)$$

Duas grandes vantagens de representar o Q-valor como uma combinação linear são evitar *overfitting*, e ser matematicamente conveniente, ter maneiras convenientes de calcular erro e funções que generalizem as decisões.

Percebe-se neste ponto uma semelhança bem grande com a forma como redes neurais profundas funcionam.

2.8 Deep Q-Learning

Agora que as técnicas aprendizado profundo e aprendizado por reforço foram apresentadas, falta falar do tipo de aprendizado obtido quando é feita a junção delas, que é o utilizado neste trabalho: **Deep Q-Learning**. Por se tratar de um tipo de aprendizado por reforço, mais precisamente *approximate Q-learning*, a inteligência artificial também será referida como agente.

Como a ideia é o agente aprender enxergando a tela e tudo que ele vê são matrizes, a primeira etapa consiste em processar essas informações para poder aprender. Ou seja, o primeiro passo é passar os *frames* da tela do jogo por uma **rede neural convolucional**. Essa etapa funciona conforme descrito na seção sobre **redes neurais convolucionais**: os *frames* são a entrada, ocorre o processamento nas camadas ocultas e, na camada de saída, cada neurônio tem um valor. Contudo, calcular o erro é diferente. Como as imagens passadas não são rotuladas e não é possível fazer isso manualmente, a IA precisa calcular o erro da saída da rede de outra forma. É nessa etapa que entra o **aprendizado por reforço**. Como explicado [anteriormente](#), aprendizado por reforço aprende sem o uso de exemplos rotulados, mas precisa que as características que a IA deve aprender estejam bem definidas. Enquanto tais características são definidas pela rede, o cálculo do erro e otimização dos pesos é feito pela parte de aprendizado por reforço.

O **cálculo do erro** é feito por uma função que, como toda função, possui um mínimo. Esse mínimo é normalmente calculado por alguma variação do **método do maior declive** ou **método do gradiente**³. Em matemática, gradiente é uma generalização de derivada para múltiplas variáveis e, portanto, aponta para a direção de maior crescimento da função sobre a qual foi aplicado no ponto dado. Método do gradiente, por sua vez, utiliza o **negativo** do gradiente para apontar para o mínimo local e, com isso, minimizar o valor da função.

Seja $F(x)$ uma função de múltiplas variáveis, x_t um ponto no instante t e α um número real que multiplica o gradiente de $F(x)$. Em contexto de aprendizado de máquina, $F(x)$ é a função de erro, x_t é o vetor de pesos na t -ésima iteração e α é a taxa de aprendizado. A redução do erro é feita atualizando os pesos da seguinte forma:

$$x_{t+1} = x_t - \alpha \nabla F(x_t) \quad (2.12)$$

Intuitivamente, começa-se em um ponto x_0 qualquer e utiliza-se esse algoritmo para deslocar-se para um ponto vizinho x_1 que, se α for pequeno o suficiente, $F(x_0) \geq F(x_1)$. Se isso for feito iterativamente, tem-se $F(x_t) \geq F(x_{t+1})$ a cada passo. Importante notar que, se o α for muito alto, a redução do erro é rápida, porém instável e pode sequer chegar perto do mínimo do erro. Por outro lado, se for muito pequeno, a redução fica precisa, mas lenta. A figura 2.4 representa essas situações.



Figura 2.4: Se α for muito alto, a diminuição se torna instável ou pode nem ocorrer (a esquerda); se for muito pequeno, se torna precisa, porém lenta (a direita). Curva representando função de erro desenhada com <https://www.desmos.com/calculator>

Existem diversos algoritmos de redução do erro e otimização dos pesos, como o *RMSProp*, *Adam*, *Adadelta*, dentre outros.

³ *Gradient descent* em inglês

2.9 Aprimorando o aprendizado

Deep Q-Learning é a base para o aprendizado da inteligência artificial deste trabalho. Porém, ao longo do tempo, foram descobertas outras técnicas que melhoram a aprendizagem do agente, seja acelerando ou ajudando a evitar decisões ruins. Nesta seção, serão apresentadas duas técnicas que ajudam a estabilizar e acelerar o aprendizado do programa: *experience replay* [Lin92] e *alvo fixo*.

2.9.1 *Experience Replay*

Por conta da forma como *Deep Q-Learning* funciona, se a rede aprendesse com os *frames* conforme o agente os vê, a entrada seria composta de estados sequenciais altamente correlacionados. Isso significa que ela se atualizaria apenas com as experiências passadas mais próximas, "esquecendo" as mais antigas. Para contornar esse problema, utiliza-se um *buffer* que armazena experiências anteriores e, a cada ação feita, ao invés de passar a transição de estados resultado dessa ação, passa-se uma amostra de experiências escolhidas aleatoriamente desse *buffer* para a rede ser atualizada. Utilizar *experience replay* também ajuda o agente a tomar ações diferentes ao invés de se prender a algumas que tiveram sucesso no passado próximo e que, possivelmente, não serão tão úteis no futuro.

2.9.2 Alvo fixo

A inteligência artificial utiliza os Q-valores tanto para decidir quais ações tomar quanto para atualizá-los na tentativa de melhor aproximar o Q-valor real. Entretanto, se o mesmo for utilizado para essas duas etapas, o aprendizado se torna instável, pois o agente não conseguirá "alcançar" o Q-valor alvo já que ele está em constante mudança. Para resolver esse problema, utiliza-se uma segunda rede neural alvo para a atualização dos Q-valores e que é atualizada de tempos em tempos, enquanto a primeira, a principal, continua sendo utilizada para escolher as ações.

Capítulo 3

Implementação

É conveniente formalizar o [MDP](#) que modela o problema antes de apresentar as arquiteturas utilizadas.

- **Gridworld:** Os estados S são o mapa em que o agente está inserido com o agente em uma das posições possível. Portanto, o número de estados existentes é igual ao número de espaços válidos. As ações possíveis A são mover-se para o espaço acima, abaixo, a direita ou a esquerda. As recompensas $R(S,A)$ são definidas pelo desenvolvedor do ambiente. No caso deste trabalho, a recompensa por chegar no objetivo gera uma recompensa de 1000 pontos, cair em uma armadilha (estado terminal de recompensa negativa) gera uma de -200 pontos, e em um estado não-terminal de -1 ponto. As probabilidades de transição $P(S, A, S')$ são as probabilidades de o agente estar em um determinado espaço do mapa (estado S) e, a partir do movimento para algum dos espaços adjacentes (ação A), chegar em algum outro espaço do mapa (estado futuro S'). Não existe aleatoriedade no movimento do agente no sentido que não é possível ele efetuar o movimento para cima, mas deslocar-se para a direita, por exemplo.
- **Pong:** Os estados S são a tela do jogo, uma matriz de 210x160x3 pixels. A parte "x3" representa o número de canais que conferem cor ao pixel. As ações possíveis A são mover a barra que o jogador controla para cima ou para baixo. As recompensas $R(S, A)$ são de +1 ponto se fizer a bola chegar no fim da tela do lado do oponente e de -1 ponto se a bola chegar no fim da tela do lado do jogador. As probabilidades de transição $P(S, A, S')$ são as probabilidades de o jogo estar em um estado S , por exemplo com a bola sendo rebatida pelo jogador, e transitar para algum outro estado futuro S' , como marcar um ponto, após tomar uma ação A , como mover a barra para cima. *Pong* é um jogo determinístico no sentido que não existe aleatoriedade na consequência das ações do jogador: se a bola colidir com a barra sempre no mesmo lugar, ela sempre será retornada na mesma direção com a mesma velocidade; marcar ponto sempre aumenta a pontuação do jogador em um. Por outro lado, existe um oponente contra o qual se está jogando e cujo comportamento configura um elemento de aleatoriedade no ambiente. Além disso, o jogador não conseguir rebater a bola como gostaria por falta de precisão também se aproxima de um elemento desse tipo.
- **Asteroids:** Os estados S são os *frames* do jogo que tem 210x160x3 pixels, cada um com três canais que determinam sua cor e intensidade, assim como no *Pong*. As ações possíveis A são mover-se para frente, girar no sentido horário, girar no sentido anti-horário, mover-se no hiper-espaço (se teletransportar para algum lugar aleatório da tela), e atirar para frente. As recompensas $R(S, A)$ são de 20 pontos por destruir um asteróide grande, 50 pontos por destruir um médio e 100 pontos por destruir um pequeno, podendo ser obtidas tanto atirando neles quanto colidindo, não havendo recompensa negativa (penalidade) por perda de vidas. As probabilidades de transição $P(S, A, S')$

são as probabilidades de o jogo estar em um estado S , por exemplo o inicial em que o jogador tem zero pontos e todas as vidas, e transitar para algum outro estado futuro S' , como destruir algum asteroide e receber pontos por isso, após tomar uma ação A , como atirar para frente. Assim como em *Pong*, *Asteroids* é um jogo determinístico no sentido que não existe aleatoriedade na consequência das ações do jogador: se ele fizer um disparo, o tiro seguirá reto durante um certo tempo até desaparecer ou atingir um asteroide; cada tamanho de asteroide sempre aumenta a pontuação do jogador pela mesma quantidade quando destruído. Os fatores mais próximos de aleatoriedade existentes no jogo são o jogador ignorar, desconhecer, abstrair e/ou não perceber partes do jogo, como a posição dos asteróides.

3.1 Arquitetura

A seguir, são descritas as arquiteturas utilizadas nos três ambientes abordados neste trabalho.

3.1.1 *Gridworld*

No caso do *Gridworld*, por ser um ambiente muito diferente do *Pong* e do *Asteroids*, teve uma arquitetura bem mais simples. O mapa tinha tamanho de 10x10, com o agente começando no canto superior esquerdo e o objetivo ficando no canto inferior direito. A rede neural convolucional tinha uma camada de convolução de 8 filtros de tamanho 2x2 e passo 1 e função de ativação ReLU seguida por uma camada *fully-connected* com um nó de saída para cada ação possível sem função de ativação. A camada convolucional utilizou inicializador de Xavier [GB10] enquanto a *fully-connected* foi inicializada com zeros nos pesos. O cálculo de erro foi feito pela função *Huber loss* [Hub64] e a otimização pela função *Root Mean Square Propagation*, mais conhecida como RMSProp [HSS14]. A função RMSProp utilizou taxa de aprendizado $\alpha = 0.05$, momentum = 0.1 (variável que indica o quanto gradientes anteriores devem ser considerados para determinar a direção do movimento) e $\epsilon = 10^{-10}$. Foram 2000 episódios de treinamento, cada um com limite de 200 ações antes de o episódio ser terminado automaticamente, *mini-batches* de tamanho 200, taxa de desconto $\gamma = 0.9$, *buffer* de memória de tamanho 200 preenchido previamente com 200 ações aleatórias. O dilema *exploration versus exploitation* utilizou $P_{ini} = 0.9$, $P_{min} = 0.4$ e $decay = 200$. A rede alvo foi atualizada a cada 200 ações.

3.1.2 *Pong*

O *Pong*, por ser mais complexo que o *Gridworld*, teve uma arquitetura mais elaborada para se obter sucesso. Primeiro, os *frames* são convertidos para escala de cinza. Em seguida, partes que não agregam informação para a IA conseguir jogar, como pontuação, foram removidos. Depois, o que sobrou da tela é redimensionado para 84x84 pixels. Essas etapas servem para reduzir o tempo de processamento ao passar pela rede convolucional e não são feitas no *Gridworld* por não haver necessidade, já que as matrizes de entrada são pequenas.

Os últimos quatro *frames* vistos são inseridos em uma fila de forma que o agente consiga captar o movimento dos objetos na tela do jogo. Esses quatro *frames* enfileirados são enviados juntos para a rede neural, de forma que a entrada tem formato 84x84x4. A primeira camada de convolução tem 32 filtros de tamanho 8x8 e passo 4, a segunda tem 64 filtros de tamanho 4x4 e passo 2, a terceira tem 64 filtros de tamanho 3x3 e passo 1. Todas elas são seguidas da função de ativação ReLU (*Rectified Linear Unit*). Depois disso, há uma camada *fully-connected* com 256 unidades e função de ativação ReLU e, por fim, outra camada *fully-connected* com um nó de saída para cada ação possível (dois neste caso), sem função

de ativação. Todas as camadas utilizam o inicializador de He ¹ [He+15] para os pesos.

Após a CNN soltar a ação escolhida, o cálculo de erro é feito pela função *Huber loss* e a otimização dos pesos é feita pelo RMSProp. O RMSProp utilizou taxa de aprendizado $\alpha = 0.00025$, momentum = 0.95 e $\epsilon = 0.01$. Foram 298 episódios de treinamento, ou aproximadamente 1 milhão de *frames*, cada um com limite 18000 ações antes de o episódio ser terminado automaticamente, *mini-batches* de tamanho 32, taxa de desconto $\gamma = 0.99$, *buffer* de memória de tamanho 1000000 que foi preenchido com 50000 ações aleatórias antes do treinamento começar. O dilema *exploration versus exploitation* utilizou $P_{ini} = 1.0$, $P_{min} = 0.1$ e $decay = 20000$. A rede alvo foi atualizada a cada 10000 ações tomadas.

Além disso, foi utilizada uma técnica simples de pular *frames* [Bel+12] para economizar tempo. O agente enxerga a tela e escolhe qual ação tomar a cada 4 *frames* ao invés de em todos os *frames*, repetindo a última ação escolhida nos *frames* pulados. Isso acelera o treinamento ao consumir menos tempo por *frame* sem prejudicar muito o aprendizado. Esse comportamento é próprio do ambiente² utilizado, não havendo partes do código destinadas a isso.

3.1.3 Asteroids

O *Asteroids* foi testado com diversas arquiteturas diferentes, maiores que as do *Pong* por ser um ambiente consideravelmente mais complexos, mas sem sucessos. Tentou-se utilizar diferentes tamanhos de redimensionamento no pré-processamento, números de filtros, tamanhos e passos, funções inicializadoras e ativadoras, unidades de saída nas camadas *fully-connected*, funções de erro, de otimização e de exploração, taxas de aprendizado, de desconto e de atualização da rede alvo, tamanho dos *mini-batches* e do *buffer* de memória. Por conta da grande gama de hiper-parâmetros a serem ajustados e o tempo consumido para treinar, os testes com este ambiente foram os mais duradouros.

Para poder demonstrar um exemplo de resultados de treinamento para o capítulo Resultados, registrou-se os resultados de um treinamento com a seguinte arquitetura. O mesmo pré-processamento do *Pong* e fileiras de quatro *frames* foi feito. A primeira camada de convolução tinha 48 filtros de tamanho 8x8 e passo 4; a segunda tinha 96 filtros de tamanho 4x4 e passo 2; e a terceira tinha 96 filtros de tamanho 3x3 e passo 1. Todas elas foram seguidas de uma função de ativação ReLU, uma camada *fully-connected* com 512 unidades e função de ativação ReLU. Por fim, uma outra camada *fully-connected* com um nó de saída para cada ação possível (cinco neste caso), sem função de ativação. Todas as camadas utilizaram o inicializador de He. O cálculo de erro foi feito pela função *Huber loss* e otimização foi feita pelo RMSProp. A taxa de aprendizado $\alpha = 0.00025$, momentum = 0.95 e $\epsilon = 0.01$. Foram 100 episódios de treinamento, ou aproximadamente 1 milhão de *frames* assim como no *Pong*, com um máximo de 100000 ações por episódio, *mini-batches* de 64, taxa de desconto $\gamma = 0.99$, *buffer* de memória de tamanho 1000000 preenchido previamente com 500 ações aleatórias. O dilema *exploration versus exploitation* utilizou $P_{ini} = 1.0$, $P_{min} = 0.1$ e $decay = 20000$. A rede alvo foi atualizada a cada 10000 ações tomadas.

Assim como no *Pong*, a técnica de pular *frames* para acelerar o treinamento foi utilizada. Porém, são pulados 3 *frames* ao invés de 4 uma vez que, no *Asteroids*, os asteróides aparecem em *frames* intercalados com os que a nave e os tiros aparecem. Utilizar 3 *frames* permite que a nave e os tiros sejam vistos pelo agente. Não existe um ambiente de *Asteroids* com esse comportamento, então ele foi implementado no código.

¹No TensorFlow, esse inicializador é chamado pelo `variance_scaling_initializer()`

²PongDeterministic-v4 do Gym

3.2 Experimentos

Os experimentos consumiram a maior parte do trabalho por poderem levar alguns minutos, no caso do *Gridworld* até mesmo horas ou dias, como no caso do *Pong* e do *Asteroids*.

3.2.1 *Gridworld*

O ambiente mais simples conseguia finalizar treinamentos de centenas de episódios em alguns minutos, e até milhares de episódios em pouco mais de uma hora por conta de suas baixas dimensões e não necessitar de arquiteturas muito grandes. Além disso, foi mais fácil analisar o aprendizado por ter poucos estados bem definido e por haver soluções evidentes de como chegar no objetivo. A análise do sucesso do agente foi feita pela sua capacidade de conseguir chegar na recompensa positiva do mapa e, em parte, pelo grau de sucesso em fazer isso ao longo do treinamento. A taxa de sucesso ao longo do treinamento, apesar de relevante, foi menos considerada por conta da alta probabilidade de se tomar uma ação aleatória a qualquer momento (mínimo de 0.4).

3.2.2 *Pong*

No caso do *Pong*, os treinamentos foram mais demorados, com episódios levando alguns minutos e passando várias horas para se perceber alguma melhoria no aprendizado. Isso se deve pelo fato de o espaço de estados ser muito maior e, mesmo com o pré-processamento feito, o de entrada para a rede neural também. Além disso, existem diversos momentos em que não há uma ação ótima bem definida a se tomar, como nos estados em que a bola viaja na direção do lado do adversário. Como os episódios só terminam quando um dos lados consegue 21 pontos (ou o número máximo de passos é excedido, o que não aconteceu neste trabalho), a avaliação foi feita pela pontuação obtida pelo agente ao final de cada partida: o mínimo possível é de -21 pontos, com o adversário marcando 21 pontos e o agente nenhum, e o máximo é de 21 pontos, sendo a situação oposta.

3.2.3 *Asteroids*

Por fim, *Asteroids* foi o ambiente mais experimentado por conta do maior número de alterações feitas nos hiper-parâmetros e nas etapas do aprendizado. Assim como no *Pong*, os treinamentos levaram várias horas, chegando a passar de um dia para o outro em algumas ocasiões. O espaço de estados é mais complexo também, com mais informações na tela em cada instante e mais ações disponíveis. A análise de sucesso foi feita de forma semelhante ao *Pong*: pela pontuação obtida ao longo do treinamento e pelo modelo construído no final. Neste ambiente, a pontuação poderia assumir qualquer valor maior ou igual a zero dentro das restrições de tempo que cada episódio tinha. Uma vez que perder vida não gera recompensa negativa e colisão com asteróides gera pontos por sua destruição, a pontuação mínima que o agente poderia obter, sem exceder o número de passos definido, é de 80 pontos, que corresponde a destruição de quatro asteróides grandes por colisão com a nave.

Capítulo 4

Resultados

Os resultados foram parcialmente como o esperado. Neste capítulo, serão descritos os resultados e porque estiveram ou não dentro das expectativas. Por conta da natureza de cada ambiente e de seus resultados, formas diferentes de avaliação foram aplicadas.

4.1 *Gridworld*

O agente se saiu muito bem no *Gridworld*, consistentemente encontrando um caminho para o objetivo com diferentes arquiteturas que não fossem drasticamente diferentes. Os gráficos não se mostraram informativos, então alguns resultados serão apresentados por uma tabela. A comparação foi feita apenas entre agente aleatório e agente treinado por *deep Q-learning*.

Jogador	% de chegadas ao objetivo
Aleatório	1.74%
DQL	66.15%

4.2 *Pong*

Já o *Pong* mostrou uma arquitetura bem mais sensível. Pequenas alterações nos hiper-parâmetros faziam o aprendizado se tornar muito mais lento ou nem acontecer. Mesmo assim, os resultados se mostraram promissores dado tempo suficiente para o agente treinar e aprender.

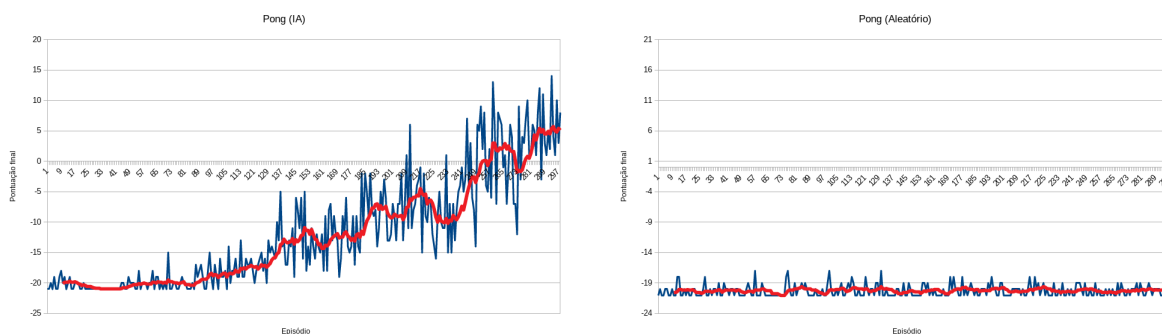


Figura 4.1: A imagem da esquerda mostra a pontuação ao longo do aprendizado e a da direita de um agente aleatório, ambos ao longo de 298 episódios. Cada episódio corresponde a uma partida. A linha azul é a pontuação por episódio enquanto a vermelha é a média dos últimos 10 episódios.

O crescimento lento, mas estável da pontuação total obtida por episódio reflete a capacidade do agente de aprender, ainda que com dificuldade, a se comportar neste ambiente de maneira positiva.

Nos experimentos, foram coletadas a pontuação final média de uma pessoa experiente após uma hora de jogo, de um agente jogando aleatoriamente, e do agente jogando segundo o modelo que montou no treinamento, todos contra a inteligência artificial padrão do *Pong*. A tabela abaixo resume os resultados obtidos.

Jogador	Pontuação média
Humano	7
Aleatório	-20.27
DQL	21

4.3 Asteroids

O *Asteroids*, por outro lado, não obteve resultados positivos nos vários testes feitos. Apesar de ser um ambiente propício para o aprendizado por *deep Q-learning*, tendo todas as informações claras na tela, ações bem definidas e recebimento de recompensas simples e consistente, o agente teve grandes dificuldades em conseguir aprender. Por conta dessas características, esperava-se que ele conseguisse aprender a se comportar nesse domínio, ainda que com dificuldade.

O gráfico abaixo exemplifica a pontuação obtida pelo agente nos treinamentos pelos quais passou e compara com a pontuação obtida por um agente aleatório.

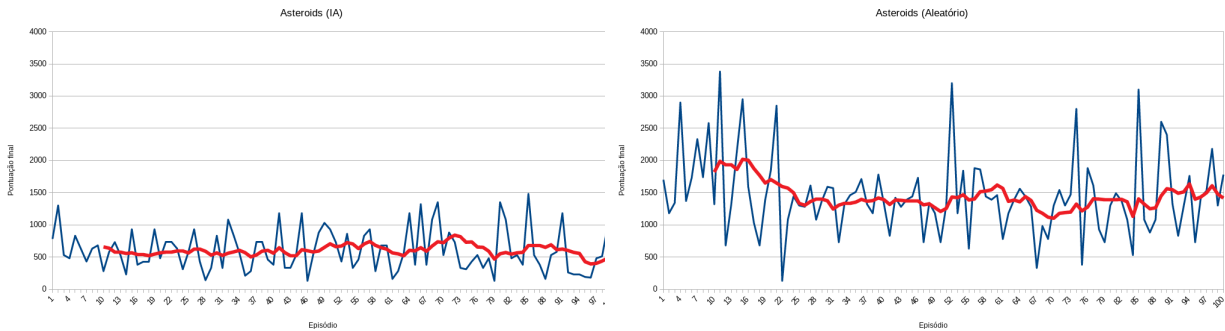


Figura 4.2: A imagem da esquerda mostra a pontuação ao longo do aprendizado e a da direita de um agente aleatório.

Percebe-se que o agente não conseguiu aprender ou sequer mostrar indícios de melhora mesmo com um tempo de aprendizado (em *frames*) próximo do *Pong*. A tabela abaixo resume a pontuação média obtida pelo agente treinado, pelo agente aleatório e por uma pessoa com pouca experiência jogando após aproximadamente uma hora de jogo. A pontuação de jogadores experientes não foi considerada por estar muito acima, passando com facilidade dos 30000 pontos.

Jogador	Pontuação média
Humano	1943.3
Aleatório	1458.1
DQL	607.8

Capítulo 5

Conclusão

Motivado pelo interesse em uma técnica de aprendizado de máquina não visto nas disciplinas de inteligência artificial da graduação, este trabalho buscou conhecer, estudar e explorar uma das formas utilizadas para ensinar um agente a se comportar em um domínio utilizando apenas imagens como entrada. Os ambientes de características e graus de complexidade distintos permitiram avaliar as capacidades e dificuldades que essa técnica apresenta, com resultados que refletiram as expectativas ainda que apenas em parte. Mesmo a falta de sucesso serviu como elemento de análise para este estudo.

O *Gridworld* apresentou sucesso consistente em encontrar um caminho até o objetivo. Isto estava dentro do esperado por conta da baixa dimensionalidade do problema: existem poucos estados, poucas ações disponíveis e não há aleatoriedade. Há poucas informações para o agente aprender, podendo inclusive ser resolvido por técnicas mais simples sem grandes problemas.

O *Pong* já se mostrou mais complicado. Ainda que seu aprendizado tenha sido [promissor](#) para os hiper-parâmetros utilizados, ele foi lento e a arquitetura é bem sensível, podendo não conseguir aprender por causa de pequenas alterações. Por possuir um espaço de estados bem maior que o *Gridworld*, mas bem menos situações diferentes e ações disponíveis que o *Asteroids*, esse resultado refletiu o grau de complexidade médio do ambiente neste trabalho: possível, mas precisa ser feito com cuidado. Um fato interessante é que, apesar de ainda haver espaço para o agente aprender, como é possível perceber no [gráfico de pontuação final do agente](#), ele obteve 21 pontos contra a IA nativa do jogo quando o modelo foi colocado a prova.

Por fim, o *Asteroids* não apresentou resultados promissores. Sendo o ambiente mais complexo dos três, com mais regras e ações para se aprender e uma variedade maior de estados possíveis, o agente não conseguiu criar um modelo que conseguisse uma pontuação boa com as arquiteturas testadas. Existem diversas técnicas que aceleram o aprendizado de *deep Q-learning* e que poderiam ser aplicadas neste ambiente para tentar obter resultados positivos. Entretanto, isso seria uma garantia somente se um conjunto de hiper-parâmetros e funções boas fosse utilizado, o que já é um obstáculo por si só considerando a quantidade que existe para serem ajustados e o tempo consumido pelos treinamentos.

Deep Q-learning apresentou resultados positivos em comparação com o que se esperava. Sua dificuldade de uso e tempo consumido são compensados pela capacidade de resolver problemas complexos com pouca influência do desenvolvedor.

Referências Bibliográficas

- [SB18] Sutton, R. S., Barto, A. G. *Reinforcement learning: an introduction*. 2nd ed. The MIT Press, 2018. ISBN: 9780262039246 9
- [HSS14] Hinton, G., Srivastava N., Swersky K. Aula 6.5 - Divide the gradient by running average of its recent magnitude. *COURSERA: Neural Networks for Machine Learning*, 4(2): 26–31. 16
- [Mni+13] Mnih, V., Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., Riedmiller, M. A. *Playing Atari with Deep Reinforcement Learning*. Em: *CoRR* (dez. de 2013). ISSN: 1312.5602. 2
- [Hub64] Huber, P. J. *Robust Estimation of a Location Parameter*. Em: *Ann. Math. Statist.* 35 (mar. de 1964), no. 1, pp. 73–101. DOI: [10.1214/aoms/1177703732](https://doi.org/10.1214/aoms/1177703732). URL: <https://doi.org/10.1214/aoms/1177703732> 16
- [He+15] He, K., Zhang, X., Ren, S., Sun, J. *Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification..* Em: *CoRR* (fev. de 2015). ISSN: 1502.01852. 17
- [Lin92] Lin, L.J. *Self-improving reactive agents based on reinforcement learning, planning and teaching.*, Em: *Machine Learning* 8(3–4) (mai. de 1992), pp. 293–321. ISSN: 1573-0565. DOI: [10.1007/BF00992699](https://doi.org/10.1007/BF00992699). URL: <https://doi.org/10.1007/BF00992699> 13
- [GB10] Glorot, X., Bengio Y. *Understanding the difficulty of training deep feedforward neural networks.*, Em: *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics* 9 (mai. de 2010), pp. 249–256. URL: <http://proceedings.mlr.press/v9/glorot10a.html>. 16
- [Bel+12] Bellemare, M. G., Naddaf, Y., Veness, J., Bowling, M. *The Arcade Learning Environment: An Evaluation Platform for General*, Em: *CoRR* 47 (jun. de 2013), pp. 253–279. ISSN: 1207.4708. URL: <https://dblp.org/rec/bib/journals/corr/abs-1207-4708>. 17