Apprentissage automatique 1 (EMINF2C1)

Cours 3 : Réseaux de neurones récurrents

Contributeur : Stergos Afantenos

Philippe Muller

Contact: prenom.nom@irit.fr

Introduction

- Lors du cours précédent nous avons vu comment nous pouvons traiter les données de taille fixe, et le cas particulier des images à l'aide des Réseaux Convolutifs (Convolutional Neural Networks, CNNs).
- La question se pose naturellement : comment pouvons nous traiter les données séquentielles qui peuvent ne pas avoir une taille fixe, comme par exemple les signaux sonores, le texte, etc?

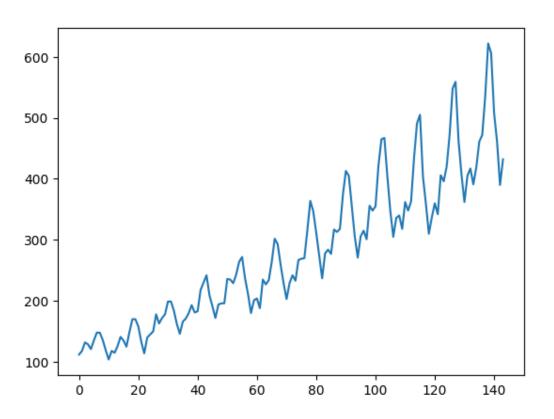
Analyse de sentiments

Loves the German bakeries in Sydney. Together with my imported honey it feels like home	Positive
@VivaLaLauren Mine is broken too! I miss my sidekick	Negative
Finished fixing my twitterI had to unfollow and follow everyone again	Negative
@DinahLady I too, liked the movie! I want to buy the DVD when it comes out	Positive
@frugaldougal So sad to hear about @OscarTheCat	Negative
@Mofette briliant! May the fourth be with you #starwarsday #starwars	Positive
Good morning thespians a bright and sunny day in UK, Spring at last	Positive
@DowneyisDOWNEY Me neither! My laptop's new, has dvd burning/ripping software but I just can't copy the files somehow!	Negative

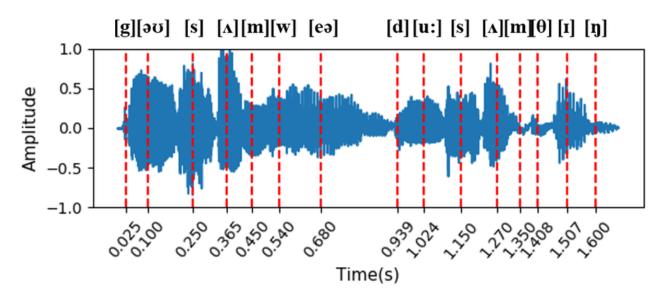


Séries temporelles

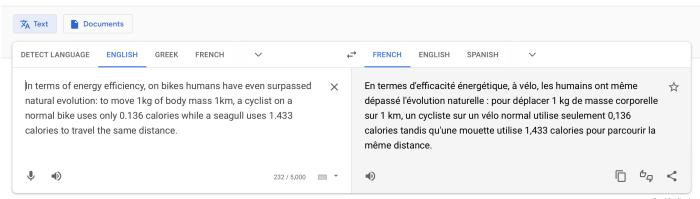
Exemple : données du trafic aérien international



Reconnaissance de la parole



Traduction automatique



Send feedback



Génération de légendes à partir d'une image

two birds sitting on top of a tree branch.

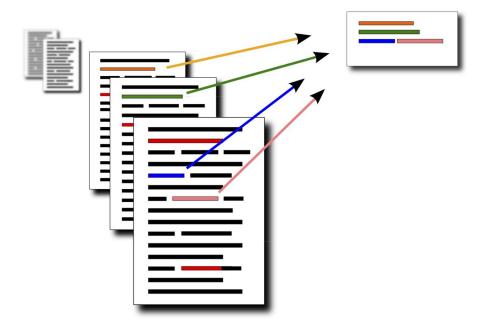


an elephant standing next to rock wall.

a man riding a bike down a road next to a

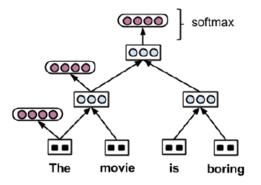
body of water.

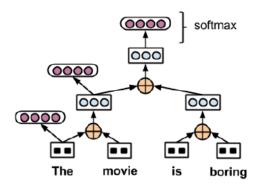
Création de résumés





Entrée structurée





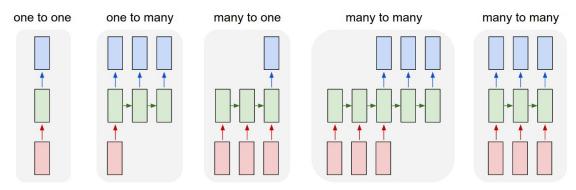


Applications pour lesquelles nous avons des données de taille variable :

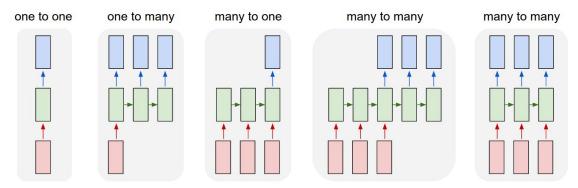
- Reconnaissance de la parole
- Traitement de données textuelles :
 - Traduction automatique
 - Création de résumés
 - Analyse de sentiments
 - •
- Génération de légendes à partir d'une image
- Vidéos
- Séries financières
- Données biologiques
- Signaux médicaux
- ..



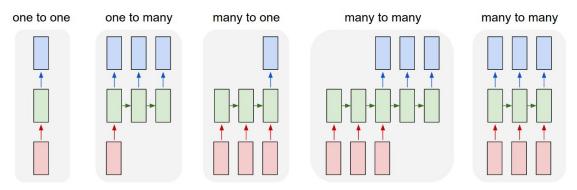
- Dans un problème "classique" nous avons un "objet" et nous voulons le classifier dans une classe, parmi un ensemble fini de classes. C'est un problème one-to-one
- Cette situation n'est pas toujours convenable, et d'autres configurations peuvent exister.



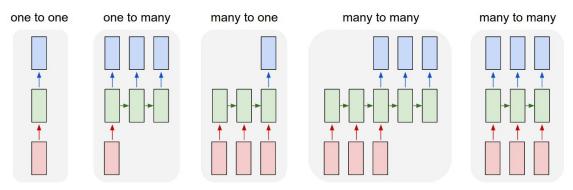
one-to-many: Prendre en entrée un objet (une image, par exemple) et produire une séquence (une légende, par exemple)



many-to-one : Prendre en entrée une séquence (un texte, par exemple) et le classifier (faire une analyse de sentiments, par exemple).



many-to-many: Prendre en entrée une séquence (un texte en français, par exemple) et produire une autre séquence (sa traduction en anglais, par exemple)



many-to-many (bis): Prendre en entrée une séquence (un signal sonore discrétisé) et produire une autre séquence pour chaque élément de l'entrée (une transcription)

Pour beaucoup de problèmes nous avons une suite de données

$$\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(\tau)}$$

et nous souhaitons produire une séquence de sortie

$$y^{(1)}, y^{(2)}, \dots, y^{(\tau)}$$

• L'idée au cœur des RNN : nous pouvons avoir un modèle séparé pour chaque $\mathbf{x}^{(i)}$ mais ensuite **partager** les paramètres entres les différents modèles via des états internes

$$\mathbf{h}^{(1)}, \mathbf{h}^{(2)}, \dots, \mathbf{h}^{(\tau)}$$

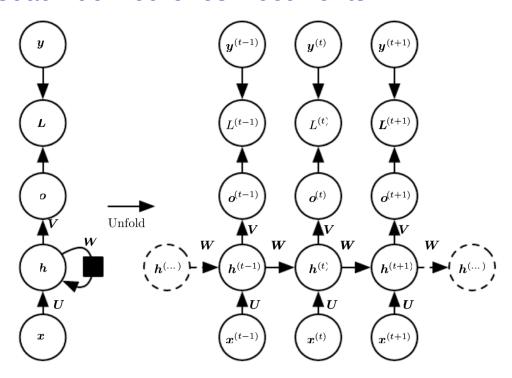


Image taken from https://github.com/janishar/mit-deep-learning-book-pdf



 Nous pouvons décrire le RNN précédent avec les équations suivantes :

$$\mathbf{h}^{(t)} = tanh(\mathbf{b} + \mathbf{W}\mathbf{h}^{(t-1)} + \mathbf{U}\mathbf{x}^{(t)})$$

$$\mathbf{o}^{(t)} = \mathbf{c} + \mathbf{V}\mathbf{h}^{(t)}$$

$$\hat{\mathbf{y}}^{(t)} = f(\mathbf{o}^{(t)})$$

où **b**, **W**, **U**; **c**, **V** sont des paramètres à apprendre.

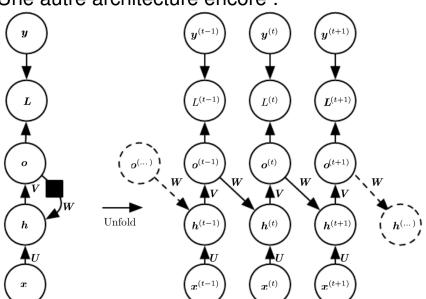
• Le RNN le plus simple est le suivant :

$$\mathbf{h}^{(t)} = tanh(\mathbf{W}\mathbf{h}^{(t-1)} + \mathbf{U}\mathbf{x}^{(t)})$$
$$\hat{\mathbf{y}}^{(t)} = f(\mathbf{V}\mathbf{h}^{(t)})$$



- Ce qui est important est que les paramètres sont partagés à travers le temps.
- ullet $\mathbf{h}^{(t-1)}$ peut également être un paramètre.

Une autre architecture encore:

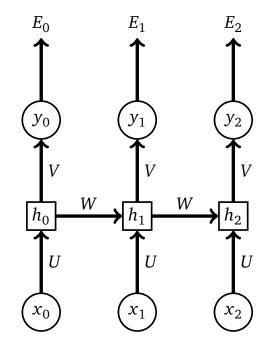


Erreur global :

$$E = \sum_{t=0}^{T} E_t$$

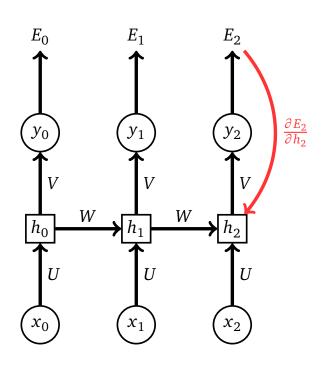
 Rétropropagation pour adapter les paramètres

$$\frac{\partial E}{\partial U} = \sum_{t=0}^{T} \frac{\partial E_t}{\partial U}$$



- Pour calculer $\frac{\partial E}{\partial U}$ nous calculons d'abord $\frac{\partial E_2}{\partial U}$
- et nous propageons l'erreur jusqu'à h_2

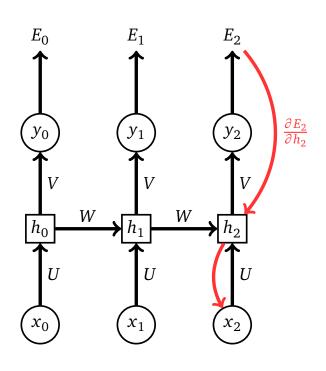
$$\frac{\partial E_2}{\partial U} = \frac{\partial E_2}{\partial h_2} \cdots$$





- Pour calculer $\frac{\partial E}{\partial U}$ nous calculons d'abord $\frac{\partial E_2}{\partial U}$
- l'erreur est ensuite propagé à U

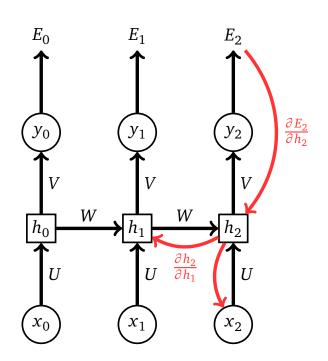
$$\frac{\partial E_2}{\partial U} = \frac{\partial E_2}{\partial h_2} (x_2^T \cdots$$





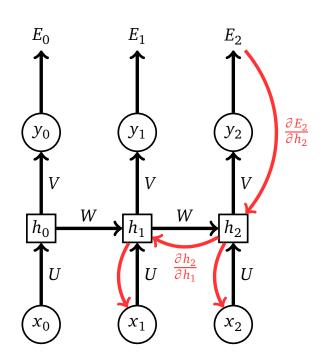
- Pour calculer $\frac{\partial E}{\partial U}$ nous calculons d'abord $\frac{\partial E_2}{\partial U}$
- Nous devons continuer à rétropropager vers h_0 et h_1

$$\frac{\partial E_2}{\partial U} = \frac{\partial E_2}{\partial h_2} (x_2^T + \frac{\partial h_2}{\partial h_1} (\cdots$$



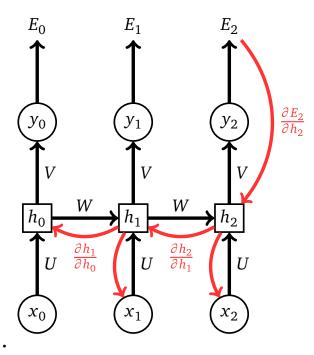
- Pour calculer $\frac{\partial E}{\partial U}$ nous calculons d'abord $\frac{\partial E_2}{\partial U}$
- L'erreur est ensuite propagé à U au premier pas

$$\frac{\partial E_2}{\partial U} = \frac{\partial E_2}{\partial h_2} (x_2^T + \frac{\partial h_2}{\partial h_1} (x_1^T \cdots$$



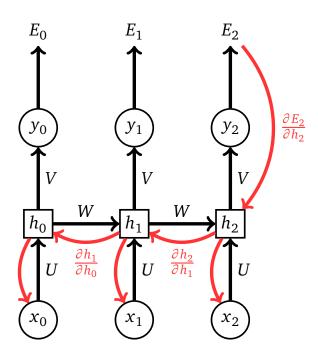
- Pour calculer $\frac{\partial E}{\partial U}$ nous calculons d'abord $\frac{\partial E_2}{\partial U}$
- et nous continuons avec h_0

$$\frac{\partial E_2}{\partial U} = \frac{\partial E_2}{\partial h_2} (x_2^T + \frac{\partial h_2}{\partial h_1} (x_1^T + \frac{\partial h_1}{\partial h_0} \cdots$$





- Pour calculer $\frac{\partial E}{\partial U}$ nous calculons d'abord $\frac{\partial E_2}{\partial U}$
- et nous finissons avec la rétropropagation sur *U* au premier pas



$$\frac{\partial E_2}{\partial U} = \frac{\partial E_2}{\partial h_2} (x_2^T + \frac{\partial h_2}{\partial h_1} (x_1^T + \frac{\partial h_1}{\partial h_0} x_0^T))$$

• Les mêmes opérations sont effectués afin de calculer $\frac{\partial E_1}{\partial U}$ et $\frac{\partial E_0}{\partial U}$ pour obtenir à la fin :

$$\frac{\partial E}{\partial U} = \sum_{t=0}^{T} \frac{\partial E_t}{\partial U}$$

 Nous devrons également calculer les gradients sur les autres paramètres :

$$\frac{\partial E}{\partial V} = \sum_{t=0}^{T} \frac{\partial E_t}{\partial V} \qquad \qquad \frac{\partial E}{\partial W} = \sum_{t=0}^{T} \frac{\partial E_t}{\partial W}$$

Comme pour les autres modèles déjà vus, les librairies de Deep Learning (torch, tensorflow) font ces opérations automatiquement.

Limites des RNN

Les problèmes auquels les RNNs font face sont les suivants :

- Dépendances à long distance
- Explosion du gradient
- Dissipation du gradient

• Question : Quelle ville est la capitale de France?

Texte pris de wikipidia et légèrement modifié.

- Question : Quelle ville est la capitale de France ?
- Paris ... est la capitale de France.

Texte pris de wikipidia et légèrement modifié.

- Question : Quelle ville est la capitale de France?
- Paris ... est la capitale de France.
- Paris, qui se situe au cœur d'un vaste bassin sédimentaire aux sols fertiles et au climat tempéré, le bassin parisien, sur une boucle de la Seine, entre les confluents de celle-ci avec la Marne et l'Oise et qui est également le chef-lieu de la région Île-de-France et le centre de la métropole du Grand Paris, créée en 2016, est la capitale de France.

Texte pris de wikipidia et légèrement modifié.

- Si on veut apprendre des dépendances à longue distance il faut être capable de propager le gradient à travers le réseau.
- Si notre séquence est longue, cette propagation peut être rapidement instable.
- Deux problèmes surviennent : explosion du gradient ou bien dissipation du gradient.

Explosion de gradient

- Si à chaque étape le gradient est amplifié, nous aurons une explosion du gradient à la fin.
- Une solution, mais qui n'est pas forcement optimale, est le gradient clipping (Pascanu et al. 2013)

$$g = \frac{\partial E}{\partial W}$$
if $||g|| \ge$ seuil then
$$g \leftarrow \frac{\text{seuil}}{||g||} g$$
end if

Dissipation du gradient

- Si l'inverse est vraie, c'est à dire qu'à chaque étape le gradient s'atténue, nous aurons une dissipation du gradient.
- L'apprentissage de dépendances à longue distance n'est pas possible.
- Une solution simple, comme avant, n'est pas possible non plus.
- Il faudra utiliser des architectures particulières pour pouvoir améliorer la performance.

Dissipation/Explosion du gradient

• Est-ce un problème spécifique aux RNNs?

Dissipation/Explosion du gradient

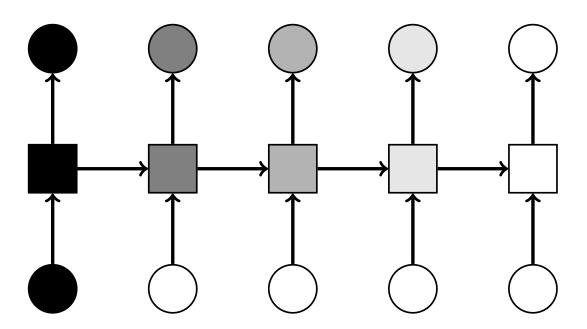
- Est-ce un problème spécifique aux RNNs?
- Non! Même les réseaux de convolution et les MLP peuvent souffrir de ce problème, surtout quand on a des couches très profondes.

Dissipation/Explosion du gradient

- Est-ce un problème spécifique aux RNNs?
- Non! Même les réseaux de convolution et les MLP peuvent souffrir de ce problème, surtout quand on a des couches très profondes.
- Une solution que beaucoup d'architectures adaptent est l'ajout de connections directes entres les couches distantes (cf connexions résiduelles cours précédent).

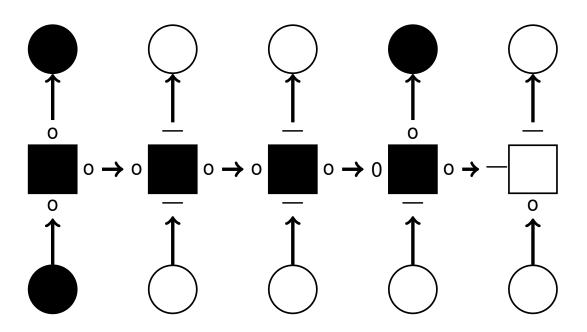
Mémoire dans le temps

Un RNN classique n'est pas capable de retenir de l'information pendant longtemps



Mémoire dans le temps

Solution: portes



Long Short Term Memory networks

Les LSTMs sont une forme de RNN qui sont capables d'apprendre des dépendances à longue distance, quelque chose que les RNNs classiques n'arrivent pas à faire très bien.

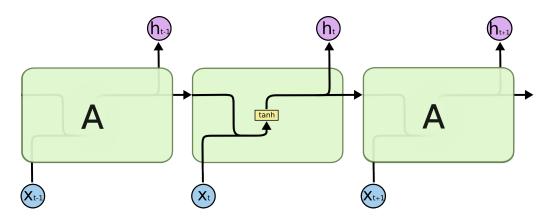


Figure 1 – Un RNN classique avec une couche

Long Short Term Memory networks

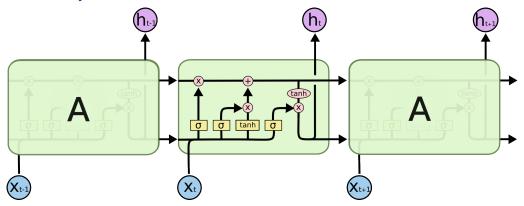
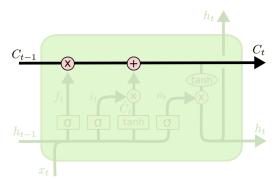


Figure 2 – Un LSTM contient 4 couches cachées qui interagissent

Long Short Term Memory networks

- L'idée principale derrière les LSTMs est le fait que nous pouvons avoir une sorte de mémoire (cell state) qui est partagée entre les différents étapes
- Cette mémoire est modifiée par quelques interactions linéaires à chaque étape via des « portes » (gates).
- Nous avons très peu d'opérations sur la cellule mémoire et l'information peut passer très facilement.



Long Short Term Memory networks

Les portes sont un moyen de permettre aux informations d'être sélectivement transmises. Elles sont composées par une couche de neurones utilisant la fonction sigmoïde et une opération de Hadamard.



La couche sigmoïde génère des valeurs entre 0 et 1. 0 signifie que rien ne passe et 1 signifie que tout passe.

Un LSTM contient 3 portes de contrôle.

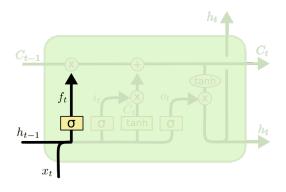
Produit Hadamard

Petit rappel

Si nous avons deux matrices $A=[a_{ij}]_{n\times m}$ et $B=[b_{ij}]_{n\times m}$ le produit Hadamard est une troisième matrice $C=[c_{ij}]_{n\times m}$ tel que

$$c_{ij} = a_{ij} \cdot b_{ij} \quad \forall i \in [1 \dots n], j \in [1 \dots m]$$

Le réseau doit d'abord déterminer ce qu'il va «oublier» (forget gate) en prenant en compte le \mathbf{h}_{t-1} et le \mathbf{x}_t



$$f_t = \sigma(\mathbf{W}_f \cdot [\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_f)$$

- σ est la fonction sigmoïde bornée entre 0 et 1.
- Ce qu'on va « oublier » concerne la cellule mémoire.

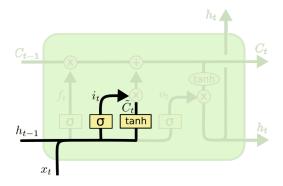
Ensuite le réseau doit déterminer les informations à retenir dans la mémoire (cell)

 D'abord une couche sigmoïde (input gate layer) décide des valeurs qui vont être misent à jour.

$$i_t = \sigma(\mathbf{W}_i \cdot [\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_i)$$

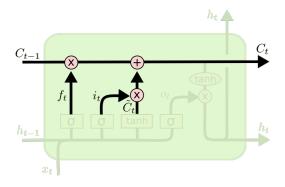
• Ensuite une couche tanh créer un vecteur de valeurs candidats $\tilde{\mathbf{C}}_t$ qui peuvent être ajoutés à la mémoire.

$$\tilde{\mathbf{C}}_t = tanh(\mathbf{W}_C \cdot [\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_C)$$



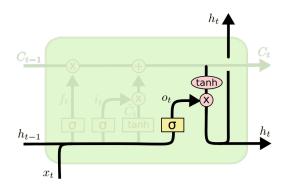


Nous pouvons donc maintenant mettre à jour la mémoire C_{t-1} pour obtenir C_t en combinant i_t et $\tilde{\mathbf{C}}_t$.



$$C_t = f_t \otimes C_{t-1} + i_t \otimes \tilde{\mathbf{C}}_t$$

- Finalement le réseau doit produire la sortie, selon C_t
- D'abord nous nous appliquons une sigmoïde pour déterminer quel morceaux de la mémoire nous allons sortir
- Ensuite nous passons C_t par une tanh (pour obtenir des valeurs entre -1 et 1) et nous multiplions par la sortie du sigmoïde



$$o_t = \sigma(\mathbf{W}_o \cdot [\mathbf{h}_{t-1}, \mathbf{x}_t] + \mathbf{b}_o)$$
$$h_t = o_t \otimes tanh(C_t)$$

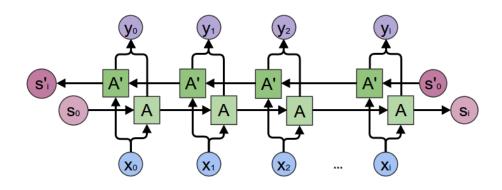
 Les LSTMs sont capables de représenter le contexte d'une entrée (un mot par exemple)

- Les LSTMs sont capables de représenter le contexte d'une entrée (un mot par exemple)
- Ce contexte est limité à gauche seulement, par contre!

- Les LSTMs sont capables de représenter le contexte d'une entrée (un mot par exemple)
- Ce contexte est limité à gauche seulement, par contre!
- Quid du contexte à droite?

- Les LSTMs sont capables de représenter le contexte d'une entrée (un mot par exemple)
- Ce contexte est limité à gauche seulement, par contre!
- Quid du contexte à droite?
- Ce n'est pas toujours possible d'avoir un contexte à droite (par exemple dans un scénario génératif), mais dans beaucoup de cas on peut y avoir accès

- Les LSTMs sont capables de représenter le contexte d'une entrée (un mot par exemple)
- Ce contexte est limité à gauche seulement, par contre!
- Quid du contexte à droite?
- Ce n'est pas toujours possible d'avoir un contexte à droite (par exemple dans un scénario génératif), mais dans beaucoup de cas on peut y avoir accès
- Solution : LSTMs Bidirectionnnels



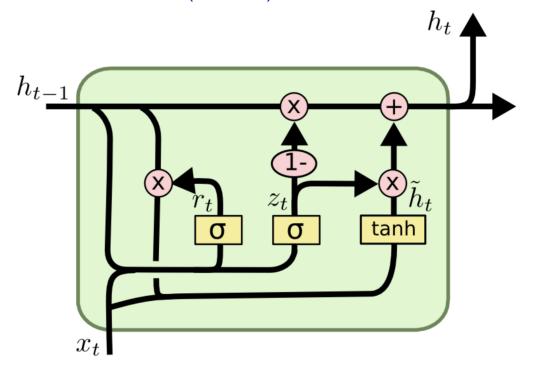
$$\overrightarrow{\mathbf{h}}_{t} = LSTM_{FW}(\overrightarrow{\mathbf{h}}_{t-1}, \mathbf{x}_{t})$$

$$\overleftarrow{\mathbf{h}}_{t} = LSTM_{BW}(\overleftarrow{\mathbf{h}}_{t-1}, \mathbf{x}_{t})$$

$$\mathbf{h}_{t} = [\overrightarrow{\mathbf{h}}_{t}; \overleftarrow{\mathbf{h}}_{t}]$$

Bien évidemment, un RNN quelconque peut être bidirectionnel

- Les GRUs est une autre architecture qui contient une mémoire permettant de capturer les dépendances à long distance
- La décision concernant les informations que le réseaux va « retenir » et les informations qu'il va « oublier » se fait via deux unités avec gates :
 - 1. une unité « update »
 - 2. une unité « reset »



Les équations pour le GRU sont les suivantes, u représente la gate pour le « update » et r pour « reset » :

$$\begin{aligned} u_t &= \sigma \left(\mathbf{b}_u + \mathbf{U}_u \mathbf{x}_t + \mathbf{W}_u h_{t-1} \right) \\ r_t &= \sigma \left(\mathbf{b}_r + \mathbf{U}_r \mathbf{x}_t + \mathbf{W}_r h_{t-1} \right) \\ h_t &= u_t \otimes tanh(\mathbf{U}_g \mathbf{x}_t + \mathbf{W}_g(r_t \otimes h_{t-1}) + \mathbf{b}_g) + (1 - r_t) \otimes h_{t-1} \end{aligned}$$

- Les GRUs sont souvent utilisés au lieu des LSTMs
- Ils n'ont pas une mémoire explicite
- Souvent on obtient des résultats similaires
- Ils sont plus rapide à calculer
- Nous pouvons avoir des GRU bidirectionnels

Question : peut-on utiliser les réseaux récursifs afin de apprendre un modèle et ensuite l'utiliser pour produire des séquences?

Question : peut-on utiliser les réseaux récursifs afin de apprendre un modèle et ensuite l'utiliser pour produire des séquences?

- Entrée : un texte (séquences de caractères UTF, par exemple, 1000 caractères)
- Sortie : Prédire le caractère suivant
- C'est une forme de modèle de langage
- Pour calculer l'erreur nous pouvons utiliser l'entropie croisée

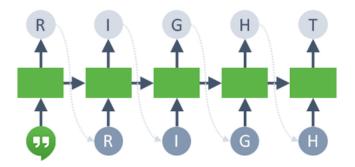


Image credit



Exemple de génération entraîné sur des textes journalistiques

- Après initialisation : usb9xkrd9ruaias\$dsaqj'4lmjwyd61/se.lcn6jey0pbco40ab'65
 8um324nqdhm<ufwt#y*/w5bt'nm.zq«2rqm-a2'2mst#u315w&tNwdqNafqh
- Après une époque d'entraînement :
 to will an apple for a N shares of the practeded to working rudle
 and a dow listed that scill extressed holding a
- Après 76 époques d'entraînement : president economic spokesman executive for securities was support to put used the sharelike the acquired who pla

c'est plus ou moins la stratégie de base des modèles de génération de texte actuels

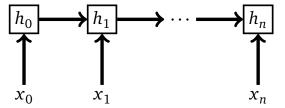
http://deeplearningathome.com/2016/10/



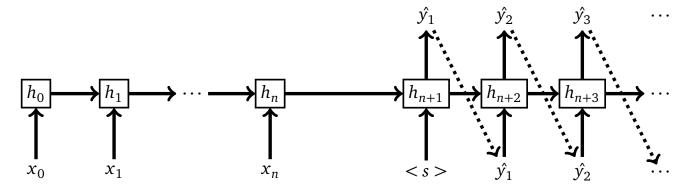
Exemple d'utilisation des RNNs génératifs

- Génération de musique
- Traduction automatique
- Production des résumés
- Génération des dialogues
- Chatbot
- Analyse syntaxique
- Génération du code (python, C, etc) à partir du langage naturel
- Génération d'écriture manuscrite
- Génération de parole

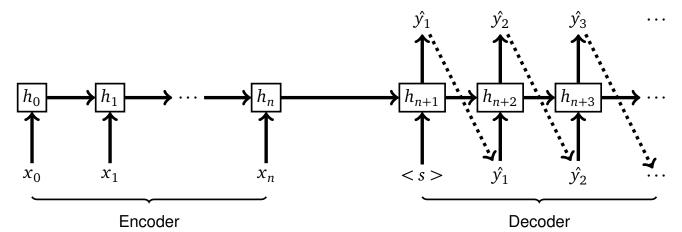
RNN génératif et le modèle Sequence to Sequence (seq2seq)



RNN génératif et le modèle Sequence to Sequence (seq2seq)



RNN génératif et le modèle Sequence to Sequence (seq2seq)



Entraînement de modèles RNNs génératifs

- Entraînement : étant donné $(x, y_{1:T})$ le modèle est entraîné en prenant toute la séquence d'un coup.
- Nous utilisons le Negative Log Likelihood (vraisemblance)

$$\mathcal{L}_{NLL}(\theta) = -\sum_{t} \log p(w_t = y_t | y_{1:t-1}, x; \theta)$$

 Test : nous avons un scénario de prédiction structuré où la structure est une séquence

$$\hat{y}_{1:T} = \underset{w_{1:T}}{\operatorname{argmax}} \sum_{t} \log p(w_t | w_{1:t-1}, x; \theta)$$

« Décodage »

- À chaque étape nous avons une distribution de probabilité sur tous les symboles (mots)
- Le problème est que nous souhaitons « décoder » ces probabilités afin de trouver la séquence les plus « intéressante » (score optimal) : mais problème combinatoire, recherche exhaustive trop couteuse.
- → Stratégies de décodage approximatives
 - Approche « glouton » (greedy search)
 - Beam search
 - Top-K sampling

Recherche exhaustive

• Nous cherchons essentiellement de maximiser (pour un taille T) :

$$P(y,x) = P(y_1|x)P(y_2|y_1,x)\cdots P(y|y_1,\cdots,y_{T-1},x)$$

$$= \prod_{t=1}^{T} P(y_t|y_1,\cdots,y_{t-1},x)$$

Recherche exhaustive

Nous cherchons essentiellement de maximiser (pour un taille T) :

$$P(y,x) = P(y_1|x)P(y_2|y_1,x)\cdots P(y|y_1,\cdots,y_{T-1},x)$$

$$= \prod_{t=1}^{T} P(y_t|y_1,\cdots,y_{t-1},x)$$

 Nous pouvons chercher exhaustivement toutes les séquences et choisir celle qui maximise le score globale

Recherche exhaustive

Nous cherchons essentiellement de maximiser (pour un taille T) :

$$P(y,x) = P(y_1|x)P(y_2|y_1,x)\cdots P(y|y_1,\cdots,y_{T-1},x)$$

$$= \prod_{t=1}^{T} P(y_t|y_1,\cdots,y_{t-1},x)$$

- Nous pouvons chercher exhaustivement toutes les séquences et choisir celle qui maximise le score globale
- Problème : Le coût est trop élevé : $O(V^T)$, V étant le vocabulaire et T la longueur de la séquence produite, c'est prohibitive.

Greedy Decoding

 Très simplement, à chaque étape nous prenons le symbol (mot) le plus probable.

$$\hat{y}_t = \operatorname*{argmax}_{w} P(w|\hat{y}_1, \dots, \hat{y}_{t-1}, x)$$

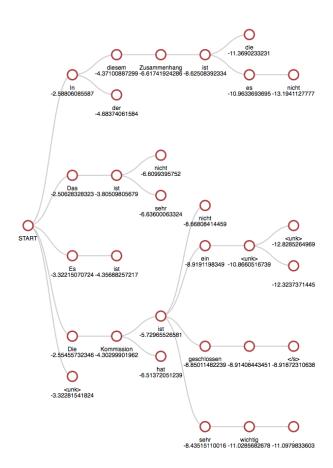
 Problème : aucun moyen de revenir en arrière ; les séquences ne font pas toujours sens.

Beam Search

L'idée de base :

- À chaque étape nous choisissons les k prédictions plus probables.
- Une arborescence commence à se développer
- À chaque étape nous n'explorons que k branches de l'arborescence
- Quand le symbole de fin arrive, nous choisissons la séquence qui maximise le score.

Beam Search



src OpenNMT



Top-k sampling

- on ne génère qu'une série, un élément à la fois
- au lieu de conserver k branches, on tire au hasard parmi les k étapes les plus probables
- donne plus de variété, ce qui est parfois souhaitable pour de la génération (ex texte)
- variante : tirer au hasard parmi les tokens de probabilité totale > p fixé ("top-p sampling")

Quiz

Lequel de ces problèmes est un problème de séquence ou qui peut être ramené à une séquence ? (sans être nécessairement la seule méthode)

- saisie intuitive (par exemple complétion de caractères, prochain mot, T9)
- reconnaissance de sons
- nettoyage d'image (inpainting)
- génération de musique