INTRODUCTION AUX RÉSEAUX DE NEURONES SÉMINAIRE APPRENTISSAGE MACHINE EN MATHÉMATIQUES

Théo Lopès-Quintas

BPCE Payment Services, Université Paris Dauphine

25 octobre 2023

APPRENTISSAGE SUPERVISÉ

FORMULATION D'UN PROBLÈME DE MACHINE LEARNING

Dans le cadre supervisé, nous avons accès à un dataset $\mathcal D$ défini comme :

$$\mathcal{D} = \left\{ (x_i, y_i) \mid \forall i \leq n, \ x_i \in \mathbb{R}^{d'}, y_i \in \mathcal{Y} \right\}$$
Nombre d'observations

Avec $\mathcal{Y} \subseteq \mathbb{R}$ pour un problème de régression et $\mathcal{Y} \subset \mathbb{N}$ dans le cadre d'une classification. Les problèmes de Machine Learning supervisé peuvent souvent s'écrire sous la forme d'une optimisation d'une fonction de perte $\mathcal{L}: \mathbb{R}^d \times \mathcal{M}_{n,d'} \times \mathbb{R}^n \to \mathbb{R}_+$ comme :

Vecteur des paramètres optimaux

$$\theta^* = \arg\min_{\theta \in \mathbb{R}} \mathcal{L}(\theta, X, y)$$

Dimension du vecteur de paramètres

Dans la suite, pour simplifier les notations, nous omettrons la dépendance de \mathcal{L} en X (matrice des informations) et y (vecteur réponse). Notons qu'en général, nous avons $d \neq d'$ et dans le cas du deep learning, très souvent d >> d'.

PRÉSENTATION

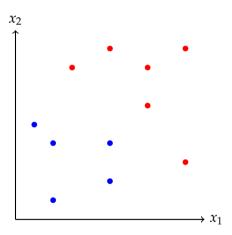


Figure – Visualisation d'un dataset pour un problème de classification avec d = 2 et $\mathcal{Y} = \{-1, 1\}$

Ici le dataset est linéairement ¹ séparable : on cherche donc à *apprendre* la droite qui permet de séparer les deux classes.

^{1.} Terme de la littérature, affine serait plus correct

PRÉSENTATION

L'algorithme du perceptron est décrit dans l'article éponyme [Minsky and Papert, 1969], on reprend ici les notations et les définitions. Le problème que l'on se pose est donc :

$$f_w(x) = \operatorname{sgn}(\langle w, x \rangle)$$

$$w^* = \operatorname{arg \, min}_{w \in \mathbb{R}^d} \sum_{i=1}^n \max \{0, -y_i \langle w, x_i \rangle\}$$

Avec f la fonction de décision finale et w le vecteur de poids définissant l'hyperplan séparateur. Le problème d'optimisation est résolu en appliquant la règle de mise à jour observation par observation :

$$w_{t+1} = w_t + yx \mathbb{1}_{y\langle w_t, x\rangle \leqslant 0}$$

VISUALISATION DE L'APPRENTISSAGE

La règle de mise à jour est :

$$w_{t+1} = w_t + yx \mathbb{1}_{y\langle w_t, x\rangle \leqslant 0}$$

Elle se visualise dans notre exemple :

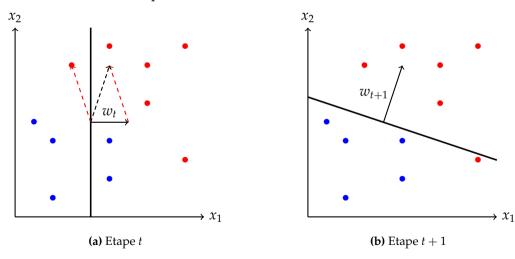


Figure – Intuition géométrique de l'apprentissage du perceptron

LA CONVERGENCE DU PERCEPTRON EST GARANTIE DANS LE CAS LINÉAIREMENT SÉPARABLE

Théorème 1 (Convergence du perceptron)

On suppose que les données issues d'un dataset \mathcal{D} soient linéairement séparables et de plus que :

$$\exists \gamma > 0, \forall i \leq n, \quad y_i \langle w^*, x_i \rangle \leq \gamma$$

On note $R = \max_{1 \le i \le n} \|x_i\|$. Alors la k-ième erreur de classification du perceptron aura lieu avant :

$$k \leqslant \left(\frac{R}{\gamma}\right)^2 \|w^*\|^2$$

 γ correspond ici à l'existence d'une *marge* qui sépare les deux classes. Ainsi, plus la marge est grande plus la k-ième erreur arrivera $t \hat{o} t$.

PREUVE

Puisque le vecteur des paramètres w n'est mis à jour que lors d'une erreur de prédiction, on note w_k le vecteur lorsque la k-ième erreur est commise. Alors :

$$w_k = w_{k-1} + y_i x_i$$

On commence par remarquer que :

$$\langle w_k, w^* \rangle = \langle w_{k-1} + y_i x_i, w^* \rangle$$

 $= \langle w_{k-1}, w^* \rangle + y_i \langle x_i, w^* \rangle$
 $\geqslant \langle w_{k-1}, w^* \rangle + \gamma$ par définition de γ

Par une récurrence immédiate, on a :

$$\langle w_k, w^* \rangle \geqslant k\gamma$$
 (1)

PREUVE

Puisqu'on veut borner le nombre d'erreurs , il faut borner l'apparition de k, et donc majorer le terme $\langle w_k, w^* \rangle$. On peut regarder l'inégalité de Cauchy-Schwarz quand on cherche à majorer de telles quantités. Pour le faire, on doit avoir une idée de la norme de w_k :

$$\|w_k\|^2 = \|w_{k-1}\|^2 + 2y_i \langle w_k, x_i \rangle + y_i^2 \|x_i\|^2$$

 $\leq \|w_{k-1}\|^2 - 2\gamma + R^2 \text{ par définition de } \gamma \text{ et } R$
 $\leq kR^2 \text{ par récurrence immédiate}$

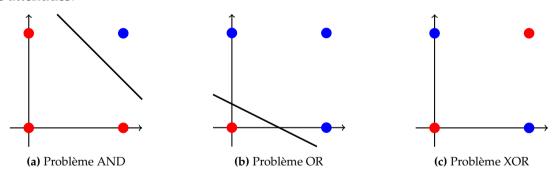
Il ne nous reste plus qu'à appliquer l'inégalité de Cauchy-Schwarz en partant de (1) :

$$k^2 \gamma^2 \leqslant \langle w_k, w^* \rangle^2$$

 $\leqslant kR^2 ||w^*||^2 \text{ par Cauchy-Schwarz}$
 $k \leqslant \left(\frac{R}{\gamma}\right)^2 ||w^*||^2$

PROBLÈME XOR

On souhaiterait savoir s'il est possible à l'aide d'un perceptron de reproduire les fonctions logiques NOT, AND, OR et XOR. Pour l'opérateur de négation, w = -1 et b = 0.5 suffisent pour renvoyer les valeurs attendues.



Dans le cas de XOR, on ne peut pas trouver un couple (w,b) qui permettent à un perceptron de séparer les classes correctement. Nous savons que XOR(A,B) = AND(NOT(AND(A,B)), OR(A,B)) donc il faudrait combiner plusieurs perceptrons pour y parvenir!

RÉSEAU DE NEURONES

EXEMPLE D'UN RÉSEAU

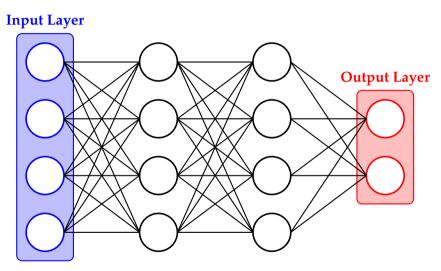


Figure – Exemple d'un réseau de neurones avec 2 couches cachées pour une classification binaire

RÉSEAU DE NEURONES

DESCRIPTION D'UN NEURONE

Un neurone renvoie un nombre après l'application d'une fonction f que l'on appelle fonction d'activation : nous reviendrons après sur cette notion.

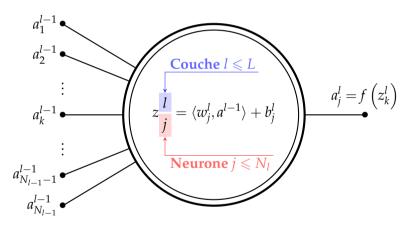


Figure – Neurone j de la couche l paramétré par les poids $w_i^j \in \mathbb{R}^{N_{l-1}}$ et le biais $b_i^l \in \mathbb{R}$

L'objectif est de comprendre comment on peut apprendre ces paramètres.

RÉSEAU DE NEURONES

DESCENTE CLASSIQUE

La méthode la plus utilisée pour résoudre ce genre de problème est la descente de gradient :

$$\theta_{t+1} = \theta_t - \boxed{\eta_t} \nabla \mathcal{L} (\theta_t)$$

Learning rate

La convergence est garantie dans le cas où \mathcal{L} est convexe. Ce n'est pas le cas dans un réseau de neurones, mais il est montré [Choromanska et al., 2015] que la majorité des minimaux locaux d'un réseau de neurones sont *proches* en terme de valeur optimale. Ainsi, obtenir un minima local est satisfaisant.

Quand on travaille avec des grands datasets, le coût de calcul/temps est grand si l'on calcule $\nabla \mathcal{L}\left(\theta_{t}\right)$ pour la totalité de la base. Ainsi, on préfère la descente de gradient **stochastique** par batch : on applique la descente de gradient à l'ensemble de la base de données en découpant en petit lots (batch) aléatoires et en mettant à jour θ à chaque fois.

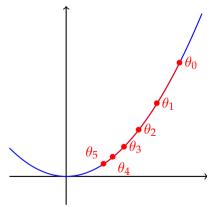


Figure – Exemple d'une descente de gradient pour $f(x) = x^2$

COMMENT CALCULER LES DÉRIVÉES PARTIELLES?

On souhaite mettre en place la descente de gradient pour pouvoir *apprendre* l'ensemble des poids. Nous avons besoin de calculer pour le neurone $j \le N_l$ à la couche $l \le L$ les gradients $\frac{\partial \mathcal{L}}{\partial w_{j,k}^l}$ et $\frac{\partial \mathcal{L}}{\partial b_j^l}$ en conservant les notations d'un neurone $j \le N_l$ à la couche $l \le L$:

$$\begin{array}{rcl} z_j^l & = & \langle w_j^l, a^{l-1} \rangle + b_j^l \\ a^{l-1} & = & f(z^{l-1}) \end{array}$$

La dernière équation étant vectorisée. Par le théorème de dérivation des fonctions composées, on obtient :

$$\frac{\partial \mathcal{L}}{\partial b_{j}^{l}} = \frac{\partial \mathcal{L}}{\partial b_{j}^{l}} \frac{\partial b_{j}^{l}}{\partial z_{j}^{l}} \quad \text{mais} \quad \frac{\partial b_{j}^{l}}{\partial z_{j}^{l}} = 1$$

$$= \frac{\partial \mathcal{L}}{\partial z_{j}^{l}}$$

$$= \frac{\partial \mathcal{L}}{\partial z_{j}^{l}}$$

$$= \frac{\partial \mathcal{L}}{\partial z_{j}^{l}}$$

$$= \frac{\partial \mathcal{L}}{\partial z_{j}^{l}}$$

$$= a_{k}^{l-1} \frac{\partial \mathcal{L}}{\partial z_{j}^{l}}$$

$$= a_{k}^{l-1} \frac{\partial \mathcal{L}}{\partial z_{j}^{l}}$$

COMMENT CALCULER LES DÉRIVÉES PARTIELLES DE LA DERNIÈRE COUCHE?

Pour le neurone $j \leq N_l$ à la couche $l \leq L$ on a obtenu que $\frac{\partial \mathcal{L}}{\partial b_j^l} = \frac{\partial \mathcal{L}}{\partial z_j^l}$ et $\frac{\partial \mathcal{L}}{\partial w_{j,k}^l} = a_k^{l-1} \frac{\partial \mathcal{L}}{\partial z_j^l}$.

On définit $\delta_j^l = \frac{\partial \mathcal{L}}{\partial z_j^l}$ la quantité commune à ces deux gradients. δ_j^l s'interprète comme l'erreur *brute*

d'un neurone. Si l'on considère les neurones les plus proches de la sortie, donc à la couche L, on a pour un neurone $j \le N_L$ avec le théorème de dérivation des fonctions composées :

$$\delta_{j}^{L} = \frac{\partial \mathcal{L}}{\partial a_{j}^{L}} \frac{a_{j}^{L}}{\partial z_{j}^{L}} \quad \text{mais} \quad a_{j}^{L} = f(z_{j}^{L})$$
$$= f'(z_{j}^{L}) \frac{\partial \mathcal{L}}{\partial a_{j}^{L}}$$

Calculer la valeur de $\frac{\partial \mathcal{L}}{\partial a_j^L}$ est aisé puisqu'il suffit de comparer la valeur prédite par le réseau à la valeur attendue. En combinant ce résultat à la question précédente, nous savons calculer la mise à jour des poids et des biais de la dernière couche.

couche l < L:

COMMENT CALCULER LES DÉRIVÉES PARTIELLES DU RESTE DU RÉSEAU?

Pour le neurone $j \leq N_l$ à la couche $l \leq L$ on a obtenu que $\frac{\partial \mathcal{L}}{\partial b_j^l} = \frac{\partial \mathcal{L}}{\partial z_j^l}$ et $\frac{\partial \mathcal{L}}{\partial w_{j,k}^l} = a_k^{l-1} \frac{\partial \mathcal{L}}{\partial z_j^l}$.

De plus, $\delta_j^L = f'(z_j^L) \frac{\partial \mathcal{L}}{\partial a_j^L}$ ce qui implique que l'on sait calculer les gradients pour les poids des neurones de la dernière couche. Pour calculer le reste des gradients, il faut probablement réussir à exprimer δ_i^L en fonction de δ_i^L : probablement de proche en proche. On considère le neurone $j \leq N_L$ à la

$$\begin{split} \delta_j^l &= \frac{\partial \mathcal{L}}{\partial z_j^l} \\ &= \sum_{k=1}^{N_l} \frac{\partial \mathcal{L}}{\partial z_k^{l+1}} \frac{\partial z_k^{l+1}}{\partial z_k^l} \quad \text{et} \quad \frac{\partial z_k^{l+1}}{\partial z_k^l} = w_{k,j}^{l+1} f'(z_j^l) \\ &= \sum_{k=1}^{N_l} w_{k,j}^{l+1} f'(z_j^l) \frac{\partial \mathcal{L}}{\partial z_k^{l+1}} \\ &= \sum_{k=1}^{N_l} w_{k,j}^{l+1} \delta_k^{l+1} f'(z_j^l) \quad \text{par d\'efinition des } \delta_j^l \end{split}$$

EXPLOSION ET DISPARITION DES GRADIENTS

Pour le neurone $j \le N_l$ à la couche $l \le L$ on a obtenu que $\frac{\partial \mathcal{L}}{\partial b_j^l} = \delta_j^l$ et $\frac{\partial \mathcal{L}}{\partial w_{j,k}^l} = a_k^{l-1} \delta_j^l$ avec

$$\delta_j^l = \sum_{k=1}^{N_l} w_{k,j}^{l+1} \delta_k^{l+1} f'(z_j^l).$$

Si l'on note $\gamma = \max_{x \in \mathbb{R}} f'(x)$ alors :

$$|\delta_j^l| \leqslant \gamma^{L-l+1} \left| \sum_{k=1}^{n_l} w_{k,j}^{l+1} \times \left(\sum_{k=1}^{n_{l+1}} w_{k,j}^{l+2} \times \left(\dots \left(\sum_{k=1}^{n_{L-1}} w_{k,j}^L \delta_j^L \right) \dots \right) \right) \right|$$

Dans les premiers réseaux de neurones la fonction sigmoid était utilisée et dans ce cas $\gamma=\frac{1}{4}$ ce qui pouvait conduire à une disparition de l'information des gradients dans les réseaux profonds. Ce phénomène est appelé *vanishing gradient*. Le phénomène inverse 2 s'appelle *exploding gradient*. Il faut donc choisir avec plus de précaution la fonction d'activation f.

^{2.} Avoir des gradients qui sont de plus en plus grand quand on remonte le réseau

FONCTIONS D'ACTIVATION

FONCTION D'ACTIVATION CLASSIQUE

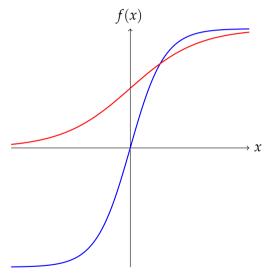


Figure – Fonctions sigmoid et tangente hyperbolique

Initialement les fonctions sigmoid et tangente hyperbolique ont été choisies pour être les fonctions d'activation dans un réseau de neurones :

$$\sigma(x) = \frac{1}{1 + e^{-x}}$$
$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

Ces deux fonctions peuvent amener à des gradients qui disparaissent ou explosent quand la back-propagation a lieu.

FONCTIONS D'ACTIVATION

FONCTION D'ACTIVATION RELU ET VARIANTES

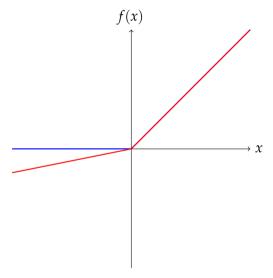


Figure - Fonctions ReLU et Leaky ReLU

Une fonction plus simple a été proposée :

$$ReLU(x) = \max\{0, x\}$$

Elle présente beaucoup moins souvent les deux phénomènes néfastes, mais en amène un autre : la mort de neurones. Puisque le gradient est fréquemment zéro, certains neurones *n'apprennent* plus. Ainsi, de nombreuses propositions ont vu le jour, dont :

Leaky ReLU(
$$x$$
) = max{ αx , x }

Avec $\alpha \geqslant 0$ un hyper-paramètre.

FONCTIONS D'ACTIVATION

FONCTIONS D'ACTIVATION MODERNE

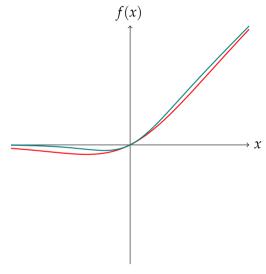


Figure – SiLU et GELU

Des variantes ont été proposé et on montré des performances équivalentes voire meilleures que ReLU sur une variété de problèmes. Nous citerons spécifiquement GELU et SiLU [Hendrycks and Gimpel, 2016].

$$\begin{array}{rcl} \operatorname{SiLU}(x) & = & x\sigma(x) & \operatorname{avec} & \sigma(x) = \frac{1}{1 + e^{-x}} \\ \operatorname{GELU}(x) & = & x\phi(x) & \operatorname{avec} & \phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} \mathrm{d}t \end{array}$$

Dans les architectures les plus poussées on observe même de nouveaux blocs dédiés à l'activation comme présenté dans [Dauphin et al., 2016] et [Shazeer, 2020].

COMMENT LIMITER LES EFFETS D'EXPLOSION OU DE DISPARITION DES GRADIENTS?

On considère un réseau de neurones à $L \in \mathbb{N}^*$ couches. On reprend la majorité des notations précédentes, mais on note z_k^l le résultat du neurone k à la couche l défini par :

Nombre de couche du réseau
$$\forall l \leqslant L, \ \forall k \in \underbrace{N_l}, \ z_k^l = \langle w_k^l, x^l \rangle$$
 Nombre de neurones de la couche l Matrice des poids du neurone k à la couche l

Nous faisons les hypothèses supplémentaires :

- ▶ Indépendance et distribution : $(w^l)_{l \leq L}$, $(x^l)_{l \leq L}$ et $(z^l)_{l \leq L}$ sont indépendants et identiquement distribués (respectivement)
- ► Indépendance : $\forall l \leq L, \ w^l \perp \!\!\! \perp x^l$
- Poids centrés : $\mathbb{E}\left[w^l\right]=0$ et la distribution est symétrique autour de 0
- lacktriangle Résultats centrés : $\mathbb{E}\left[z^l\right]=0$ et la distribution est symétrique autour de 0

On souhaite obtenir une bonne propagation des signaux dans les deux sens afin d'éviter une explosion ou une disparition des gradients. Formellement :

$$\forall l \leqslant L, \ \mathbb{V}\left[z^l\right] = \mathbb{V}\left[z^1\right] \tag{2}$$

CAS D'UNE FONCTION D'ACTIVATION IMPAIRE

Calculons pour le neurone $j \leq N_l$ à la couche $l \leq L$:

$$\mathbb{V}\left[z_{j}^{l}\right] = \mathbb{V}\left[\left\langle w_{j}^{l}, x^{l}\right\rangle\right]$$

$$= n_{\mathrm{input}}\mathbb{V}\left[w_{j,k}^{l} x_{k}^{l}\right] \quad \text{par indépendance et car identiquement distribués, pour } k \leq n_{\mathrm{input}}$$

$$= n_{\mathrm{input}}\left(\mathbb{V}\left[w_{j,k}^{l}\right]\mathbb{V}\left[x_{k}^{l}\right] + \mathbb{E}\left[w_{j,k}^{l}\right]^{2}\mathbb{V}\left[x_{k}^{l}\right] + \mathbb{E}\left[x_{k}^{l}\right]^{2}\mathbb{V}\left[w_{j,k}^{l}\right]\right)$$

$$= n_{\mathrm{input}}\mathbb{V}\left[w_{j,k}^{l}\right]\mathbb{E}\left[\left(x_{k}^{l}\right)^{2}\right] \quad \text{car } \mathbb{E}\left[w_{j,k}^{l}\right] = 0$$

Rappelons que $x^l = f\left(z^{l-1}\right)$ avec f la fonction d'activation entre la couche l-1 et la couche l. Si f est impaire, alors $\mathbb{E}\left[x^l\right] = \mathbb{E}\left[f\left(z^{l-1}\right)\right] = 0$ donc $\mathbb{E}\left[\left(x_j^l\right)^2\right] = \mathbb{V}\left[z_j^{l-1}\right]$. Ainsi,

$$\forall l \leqslant L, \forall j \leqslant N_l, \ \mathbb{V}\left[z_j^l\right] = n_{\text{input}} \mathbb{V}\left[w_{j,k}^l\right] \mathbb{V}\left[z_j^{l-1}\right] = \prod_{i=1}^{l-1} \left(n_{\text{input}} \mathbb{V}\left[w_{j,k}^l\right]\right) \mathbb{V}\left[z_j^1\right]$$

Une condition suffisante pour que l'on respecte l'équation (2) est que $\mathbb{V}\left[w_{j,k}^l\right] = \frac{1}{n_{\text{input}}}$

CAS D'UNE FONCTION D'ACTIVATION IMPAIRE

Nous venons de reproduire le raisonnement de l'article [Glorot and Bengio, 2010]. Pour résoudre le problème final, choisir la condition qui conviendra pour les deux passes (forward et backward), les auteurs proposent de prendre la moyenne entre les deux conditions. Plus tard, nous ferons références au nombre de neurones de la couche précédente (respectivement suivante) par fan in (respectivement fan out).

Notons que nous n'avons supposé aucune loi pour l'initialisation des poids à part des conditions d'indépendances, distributions et que la loi doit être symétrique autour de 0 et d'espérance 0. Les cas les plus classiques sont :

- ► Normale : $\mathcal{N}(0, \sigma^2)$: $\sigma = \sqrt{\frac{2}{\text{fan in + fan out}}}$ ► Uniforme : $\mathcal{U}([-a, a])$: $a = \sqrt{\frac{6}{\text{fan in + fan out}}}$

CAS DE LA FONCTION ReLU

Puisque cette fois f n'est pas impaire mais égale à $f(x) = \max\{0, x\}$, nous avons que :

$$\mathbb{E}\left[x^2\right] = \mathbb{E}\left[f(z)^2\right]$$

$$= \int_{-\infty}^{+\infty} f(t)^2 p(t) dt \text{ avec } p \text{ la densit\'e de probabilit\'e associ\'e à } z$$

$$= \int_{0}^{+\infty} t^2 p(t) dt$$

$$= \frac{1}{2} \mathbb{V}\left[z\right]$$

Nous avons donc cette fois:

$$\forall l \leqslant L, \forall j \leqslant N_l, \ \ \mathbb{V}\left[z_j^l\right] = \frac{n_{\mathrm{input}}}{2} \mathbb{V}\left[w_{j,k}^l\right] \mathbb{V}\left[z_j^{l-1}\right] = \prod_{i=1}^{l-1} \left(\frac{n_{\mathrm{input}}}{2} \mathbb{V}\left[w_{j,k}^l\right]\right) \mathbb{V}\left[z_j^1\right]$$

A nouveau, une condition suffisante pour que la relation (2) soit vérifée pour la passe forward est :

$$\mathbb{V}\left[w_{j,k}^l\right] = \frac{2}{n_{\text{input}}}$$

CAS DE LA FONCTION ReLU

C'est très proche de la condition quand l'on considère une fonction d'activation impaire, mais cela résulte en un écart significatif lors de l'entraînement. Le raisonnement suivi a été décrit dans l'article [He et al., 2015].

Contrairement à la résolution proposée par Xavier Glorot et Yoshua Bengio, la valeur de la variance pour les poids est obtenue en sélectionnant le *fan in* ou le *fan out* : on le note *fan mode*.

- Normale : $\mathcal{N}(0, \sigma^2)$: $\sigma = \sqrt{\frac{2}{\text{fan mode}}}$
- ► Uniforme : $\mathcal{U}([-a,a])$: $a = \sqrt{\frac{6}{\text{fan mode}}}$

On peut obtenir des distributions précises également pour le Leaky ReLU.

BIBLIOGRAPHIE I

Choromanska, A., Henaff, M., Mathieu, M., Arous, G. B., and LeCun, Y. (2015). The loss surfaces of multilayer networks. In *Artificial intelligence and statistics*. PMLR.

Dauphin, Y. N., Fan, A., Auli, M., and Grangier, D. (2016). Language modeling with gated convolutional networks. In *International conference on machine learning*, pages 933–941. PMLR.

Glorot, X. and Bengio, Y. (2010).

Understanding the difficulty of training deep feedforward neural networks.

In *Proceedings of the thirteenth international conference on artificial intelligence and statistics*, pages 249–256.

JMLR Workshop and Conference Proceedings.

He, K., Zhang, X., Ren, S., and Sun, J. (2015).

Delving deep into rectifiers: Surpassing human-level performance on imagenet classification.

In *Proceedings of the IEEE international conference on computer vision*, pages 1026–1034.

Hendrycks, D. and Gimpel, K. (2016). Gaussian error linear units (gelus). arXiv preprint arXiv:1606.08415.

BIBLIOGRAPHIE II

- Minsky, M. and Papert, S. (1969). Perceptrons.

 MIT press.
- Shazeer, N. (2020).
 Glu variants improve transformer.
 arXiv preprint arXiv:2002.05202.