

Universal Approximator Theorem: Let $\phi(\cdot)$ be a non-constant, bounded and monotonically increasing fn. $\forall \epsilon > 0$ and any continuous $f_n \in \mathbb{R}^m$, there exists an integer N , real constants $v_i b_i \in \mathbb{R}$ and real vectors $w_i \in \mathbb{R}$ where $i = 1, \dots, N$ such that: $F(\vec{x}) = \sum_{i=1}^N v_i \phi(w_i^T \vec{x} + b_i)$ with $ F(\vec{x}) - f(\vec{x}) < \epsilon$ and where ϕ is a sensible activation function. Problems: ϵ can be very large in practice, making approximation less useful, and curse of dimensionality.	
Shift Invariance: The unchanging response when the input is shifted. For classifier f and shift operator S_v , $f(\vec{x}) = f(S_v \vec{x})$ (no matter how the input is transformed, the output should remain constant) generalizes for unseen data.	Shift Equivariance: applying the shift operator after the function yields the same results as applying the function after the shift. i.e. $S_v \circ f(\vec{x}) = f(\vec{x}) \circ S_v$. It is about consistent transformation.
Translation Invariance: shift in input should have a predictable shift in hidden representation (location shouldn't matter) Locality: we should not have to move far from location (i, j) to learn valuable information to asses what the area contains.	
Fully connected net: every input feature n in an image influences ever neuron in the next layer: $n \times n$. Sparsely connected net: each neuron n is connected to a subset of neurons $k: k \times n$. Weight sharing net: weights are reused in a network	
Convolution: $(f * g)(t) = \int_{-\infty}^{\infty} f(\tau)g(t - \tau)d\tau$ for $f, g: [0, \infty] \rightarrow \mathbb{R}$ Correlation: $(f * g)(t) = \int_{-\infty}^{\infty} f(\tau)g(t + \tau)d\tau$ for $f, g: [0, \infty] \rightarrow \mathbb{R}$ commutative: $f * g = g * f$, associative $(f * g) * h = f * (g * h)$ distributive: $f_1 * (f_2 + f_3) = f_1 * f_2 + f_1 * f_3$	$M = \left\lfloor \frac{M+2 \times P-D \times (K-1)-1}{S} + 1 \right\rfloor$
Activation Fns: introduce non-linearity for more complex data learning. Unbounded outputs lead to numerical instability in training. High values cause issues with gradients leading to problems like exploding gradients. Linear: $f(x) = c \cdot x$ network behaves single-layered model. Regression. Sigmoid: $f(x) = \frac{e^x}{1+e^x}$ more analogue continuous output than step, smooth gradient between (-2,2) rapid learning between there. Vanishing gradient problem. Good for n-classifiers. Tanh: $f(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$ stronger gradient, outputs are zero-centred on avg. Vanishing gradient problem, requires good normalization. ReLU: $f(x) = \max(0, x)$ produces sparse activations, comp. Efficient (less dense activations), Dying ReLU problem often outputting 0. Leaky ReLU: $f(x) = \begin{cases} x & \text{for } x \geq 0 \\ 0.01 \cdot x & \text{for } x < 0 \end{cases}$ like ReLU – dying problem	standard CNNs are not naturally equivariant to rotations; Harmonic Networks/H-Nets; replacing kernel w/ 'circular harmonics'; rotation results in a proportionate rotation in the output.
LeNet: convolutions + avg pooling + fully connected last layer (small number of classes make this ok) performs object localization + recognition. AlexNet: + dropout after 2 layers for robustness/regularization, ReLU, maxpool (more shift invariance, keep salient features, discard less useful), softmax for classification, increased kernel size, data augmentation, model ensemble, originally split into two streams due to hardware limitations. VGG: bigger, didn't add more dense layers, didn't add more convolutional layers, but grouped layers into parametrized blocks. Using lots of narrow convolutions outperforms few wider ones, slower than others but performance is much better Inception: introduces parallel dataflow, improves performance with width and depth. ↑size=↑params=↑overfitting=↑comp resource. Patch alignment issues fixed with 1x1, 3x3 (1-padding) and 5x5 (2-padding). Naive version also includes a 3x3 maxpool in parallel for additional benefit. Detailed approach includes 1x1 convolutions to compute reductions before expensive 3x3 and 5x5. Channel size: 1x1 = 64 ch, (1x1=96ch → 3x3=128ch), (1x1=16ch → 5x5=32ch), (3x3 maxpool → 1x1=32ch) because big kernels already come with large parameter count. √ It has low param count and FLOPs: $\left[k^2 \right]^{fixed} \times c_{in} \times c_{out} \times \left[m_h \times m_w \right]^{fixed}$ implies that $\left[c_{in} \times m_h \times m_w \right]^{fixed} \times \sum_{j \in paths} (k_j^2 \times c_{out,j})$ By varying no. chan and k we optimize network performance.	
ResNet: parameterizes around an identity function instead of 0 function; you don't have to learn the identity function from scratch, allows for the addition of new layers without disrupting the outputs of previous layers. 3X3 → Batchnorm → ReLU → 3x3 → BatchNorm → combine with identity/1x1 → ReLU. DenseNet: each layer gets the feature maps from all the preceding layers (taylor expansion style), efficient and less parameters, alleviate the vanishing gradient problem by improving the gradient flow through the network, making optimization easier, scalable, since you can easily adjust the number of layers. Occasionally need to reduce resolution (transition layer) SqueezeNet: uses attention, Squeeze global average pool, fed into a Descriptor (small fully-connected NN) capture which channels are more important given the current global context of the image. Use descriptors to Excite and scale the original channels <i>Re-weight channels</i> if certain channels need to be emphasized certain features Outcomes: Dense layers are computationally and memory intensive. Real-world problems with big input tensors and many classes will prohibit their use, 1x1 convolutions act like pixel-wise multi-layer perceptron,	
BatchNorm: during GD, Each layer's learning destabilizes the next, causing a slow convergence process that takes a long time for all layers to adapt properly. BatchNorm normalizes the features within each mini-batch, thereby stabilizing the training process and speeding up convergence. $\mu_B = \frac{1}{ B } \sum_{i \in B} x_i$ $\sigma_B^2 = \frac{1}{ B } \sum_{i \in B} (x_i - \mu_B)^2 + \epsilon$ therefore $x_{i+1} = \gamma \frac{x_i - \mu_B}{\sigma_B} + \beta$ where γ, β are learnable parameters var and mean to scale and shift. BatchNorm is effectively acting as a form of regularization by introducing noise into the model. Insert after conv but before activation. Perform one batchnorm per channel, and in FCL one normalization for all. Not recommended for use with dropout. U-Net: combination of 3x3 convs with ReLU x2 + maxpool 2x2 ... up-conv 2x2 + conv 3x3 x 2 + skip connections + BatchNorm. 3D-U-Net: H-DenseUNet; specific segmentation task Unet++ ; more powerful medical imaging+uses densely connected subnetworks nnU-Net auto	
DataAugmentation: increases size and diversity of training set through artificial upsampling, e.g. random (flip, scale, rot, intensity/contrast var, cropping/padding, noise, affine/perspective transformations). Useful for anomaly detection, latent space measurement, input reconstruction,	
Supervised: learn function $x \rightarrow y$ given $p_{data}(x, y)$. Unsupervised: learn a probabilistic model which describe hidden structure $p_\theta(x) = p_{data}(x)$ Generative Latent Models: $z \approx p_\theta(z)$, $x \approx p_\theta(x z) \rightarrow p_\theta(x) = \int p_\theta(x z)p_\theta(z)dz$ where z is unobserved latent var and x is observed var. PCA: explain the variability in data as k orthogonal directions that capture most of the variance in the data. Probabilistic PCA: $p(z) = \mathcal{N}(z; 0; I)$ $z \in \mathbb{R}^K$, $K < d$, $p_\theta(x z) = \mathcal{N}(x; Wz, \theta^2 I)$, $x \in \mathbb{R}^d$ and optimise $\theta = W \in \mathbb{R}^{d \times K}$ by training with max log-likelihood, W contains K eigenvectors Clustering: $p_\theta(z) = \text{Categorical}(\pi)$, $\pi = (\pi_1, \dots, \pi_k)$, $\pi_i = p_\theta(z = i)$ and $\sum_{i=1}^K \pi_i = 1$, $p_\theta(x z) = \mathcal{N}(x; \mu_z; \Sigma_z)$	
Loss: how well your network is doing, quantifying Δ (predicted outputs, ground truth). Backprob updates model parameters, aiming to min. error. L2-norm: $\ell(x, y) = l_n = (x_n - y_n)^2$ regression. L1-norm: $\ell(x, y) = l_n = x_n - y_n $ sensitive to outliers, not differentiable Smooth L1: $\sum_i z_i$, $z_i = \begin{cases} 0.5(x_i - y_i)^2, & \text{if } x_i - y_i < 1 \\ x_i - y_i - 0.5, & \text{otherwise} \end{cases}$ for errors close to zero, it behaves like the L2 loss, else L1. Robust to outliers. Negative Log-likelihood: $\ell(x, y) = \mathcal{L} = \{l_1, \dots, l_N\}^T$, $l_n = -w_{y_n} x_n y_n$, $w_c = \text{weight}[c] \cdot \{1 \text{ if } c \neq \text{ignore}_{index}\} \cdot \{y, x\} = \begin{cases} \sum_{n=1}^N \frac{1}{\sum_{n=1}^N l_{n_i}} l_{n_i} & \text{if reduction = mean} \\ \sum_{n=1}^N l_{n_i} & \text{if reduction = sum} \end{cases}$ element-wise, weights assign importance, Cross-entropy: $\text{loss}(x, \text{class}) = -\log(\frac{e^{x[\text{class}]}}{\sum_{c \in \mathcal{C}} e^{x[c]}}) = -x[\text{class}] + \log(\sum_j e^{x[j]})$ n-classification, weighted classes optional Binary cross-entropy: $\ell(x, y) = \mathcal{L} = \{l_1, \dots, l_N\}^T$ $l_n = -w_n \text{truth}_n \cdot \log x_n + (1 - y_n) \cdot \log(1 - x_n)$, x_n predicted positive, y_n ground truth (0,1), w_n weight. Binary/Multi classification Kullback-Libler $\ell(x, y) = \mathcal{L} = \{l_1, \dots, l_N\}^T$, $l_n = y_n \cdot (\log y_n - x_n)$ suitable when target is 1-hot, suffers with numerical stability issues Margin Ranking Loss/Ranking Losses/Contrastive Loss: $\text{loss}(x, y) = \max(0, -y \cdot (x_1 - x_2) + \text{margin})$ useful to push classes as far away as possible Triplet Margin Loss: $l_n(x_0, x_p, x_n) = \max(0, m + f(x_0) - f(x_p) - f(x_0) - f(x_n))$ make samples from same classes close and different classes far away e.g. Siamese Networks Cosine Embedding Loss $\text{loss}(x, y) = \begin{cases} a - \cos(x_1, x_2), & \text{if } y = 1 \\ \max(0, \cos(x_1, x_2) - \text{margin}), & \text{if } y = -1 \end{cases}$	prior $p(\theta x) = \frac{p(\theta) \cdot p(x \theta)}{p(x)}$ evidence $p(\theta x) = \frac{p(\theta) \cdot p(x \theta)}{p(x)}$ Jensen's Inequality: if f is $\frac{d^2}{dx^2} \geq 0$ then $\forall p(x)$ $p_\theta(x) = \int p_\theta(x z)p(z)dz \geq \mathcal{N}(x; G_\theta(z), \sigma^2 I)$ where G is the neural network transform. Since $\mathbb{E}_{p(x)}[f(x)] \geq f(\mathbb{E}_{p(x)}[x])$
VAE: we want to minimise divergence between prediction and actual: $\theta^* = \arg \min D[p_{data}(x) p_\theta(x)]$. Divergence is valid iff when $D=0 \rightarrow p=q$ and ≥ 0 otherwise. We set $D = \text{Kullback-Libler divergence}$: $KL[p q] = \int p(x) \log_e \frac{p(x)}{q(x)} dx$ $\theta^* = \arg \max_{\theta} \frac{1}{N} \sum_{n=1}^N \log p_\theta(x_n)$ by using empirical risk (computing expectation w.r.t empirical measure). Fit $p(z) = \mathcal{N}(z; 0; I)$ $\wedge p_\theta(x z) = \mathcal{N}(x; G_\theta(z), \sigma^2 I)$ where G is the neural network transform. Since $p_\theta(x) = \int p_\theta(x z)p(z)dz \geq \mathcal{N}(x; G_\theta(z), \sigma^2 I)$ we need to calculate the integral over the joint distribution over the latent variable z ; not tractable. Optimize the Variational Lower Bound by $\log p_\theta(x) \geq \mathbb{E}_{q(z)}[\log p_\theta(x z)] - KL[q(z) p(z)] := \mathcal{L}(x, q, \theta)$ which is what we try to maximise. The gap between the two is the KL divergence; therefore the lowerbound improves as $q(z)$ approaches to the exact posterior. Variational Auto Encoders Since the exact posterior $p_\theta(z x)$ depends on x , the variational lower-bound is tight when $q_n(z_n) \approx p_\theta(z_n x_n)$. Therefore, we define q to be the encoder: $q(z) := q_\phi(z x)$. Therefore the objectives become: $\theta^*, \phi^* = \arg \max_{\theta, \phi} L(\phi, \theta)$ and $L(\phi, \theta) := \mathbb{E}_{p_{data}(x)}[\mathbb{E}_{p_\theta(z x)}[\log p_\theta(x z)] - KL[q_\phi(z x) p(z)]]$ where q is defined by a NN as $q_\phi(z x) = \mathcal{N}(z; \mu_\phi(x), \text{diag}(\sigma_\phi^2(x)))$ where $\mu_\phi(x)$, $\log \sigma_\phi(x) = NN_\phi(x)$. KL term has an analytical solution: $KL[q_\phi(z x) p(z)] = \frac{1}{2}(\ \mu_\phi(x)\ _2^2 + \ \sigma_\phi(x)\ _2^2 - 2(\log \sigma_\phi(x), 1) - d)$. Reparameterization: this is still expensive to calculate because $\mathbb{E}_{p_\theta(z x)}[\log p_\theta(x z)]$ requires passing every z through the generative network. Therefore, use Monte-Carlo estimation to approximate the expected log likelihood. $\mathbb{E}_{p_\theta(z x)}[\log p_\theta(x z)] \approx \log p_\theta(x z)$, where $z \sim q_\phi(z x)$ thus $\nabla_\phi L(x, \phi, \theta) \approx \nabla_\phi \mathbb{E}_{q_\phi(z x)}[\log p_\theta(x z)] - \nabla_\phi K L[q_\phi(z x) p(z)]$ and $z \sim q_\phi(z x) \iff z = \mu_\phi + \sigma_\phi \odot \epsilon$, $\epsilon \sim \mathcal{N}(\epsilon; 0; I)$ then set $z = T_\phi(x, \epsilon)$ to make $\mathbb{E}_{p_\theta(z x)}[\log p_\theta(x z)] \approx \log p_\theta(x T_\phi(x, \epsilon))$. KL annealing is when you have beta parameter in-front of KL term in loss function.	
GAN: constructs a binary classification task to assist learning generative model distribution $p_\theta(x)$ to fit the data distribution $p_{data}(x)$. Objective is: $\min_\theta \max_\phi L(\theta, \phi) := \mathbb{E}_{p_{data}(x)}[\log D_\phi(x)] + E_{p_\theta(x)}[\log(1 - D_\phi(x))]$ i.e. log(real 1) + log(fake 0). Assuming the discriminator network D_ϕ has infinite capacity with fixed θ : $\phi^* = \max_x L(\theta, \phi)$ satisfies $D_{\phi^*}(x) = \frac{p_{data}(x)}{p_{data}(x) + p_\theta(x)}$ and substituting you get the Jensen-Shannon divergence $KL[p_{data}(x) \tilde{p}(x)] + KL[p_\theta(x) \tilde{p}(x)] - 2 \log 2$ where $\tilde{p}(x) = \frac{1}{2}p_{data}(x) + \frac{1}{2}p_\theta(x)$ and thus $2JS[p_{data}(x) p_\theta(x)] - 2 \log 2$. We need to solve the 2 player game with a Double loop optimisation : with fixed theta optimise phi, $\max_\phi \mathbb{E}_{p_{data}(x)}[\log D_\phi(x)] + \mathbb{E}_{p_\theta(x)}[\log(1 - D_\phi(x))]$. With fixed phi, optimize theta $\min_\theta \mathbb{E}_{p_\theta(x)}[\log(1 - D_\phi(x))]$. loop until convergence. Usually, these are batched: $\mathbb{E}_{p_{data}(x)}[\log D_\phi(x)] \approx \frac{1}{M} \sum_{m=1}^M \log D_\phi(x_m)$, $x_m \sim p_{data}(x)$ and $\mathbb{E}_{p_\theta(x)}[\log(1 - D_\phi(x))] \approx \frac{1}{K} \sum_{k=1}^K \log(1 - D_\phi(G_\theta(z_k)))$, $z_k \sim p(z)$. Initialisation issue: generator very bad in beginning, so loss is 0. Instead, use an alternative "non-saturate" loss: $\min_\theta - \mathbb{E}_{p_\theta(x)}[\log D_\phi(x)]$ this maximises the probability of making a wrong decision on fake data. Wasserstein GAN: instead scores data. The original approach ($\min_\theta \max_\phi \mathbb{E}_{p_{data}(x)}[D_\phi(x)] - \mathbb{E}_{p_\theta(x)}[D_\phi(x)]$) doesn't consider infinite capacity of the discriminator network (which should return infinity if a real image). This makes a spiky function. We therefore constrain the lipschitz constraint $\ D_\phi(\cdot)\ _L \leq 1$. Once again, after intractability issues: $\min_\theta \max_\phi \mathbb{E}_{p_{data}(x)}[D_\phi(x)] - \mathbb{E}_{p_\theta(x)}[D_\phi(x)] + \lambda \mathbb{E}_{\tilde{p}(x)}[\ \nabla_x D_\phi(x)\ _2 - 1]^2$.	
Conditional Latent Models: the goal is to learn $p_\theta(x y)$, instead of training C separate models for C classes (doesn't generalise to continuous) make latent var and condition as input to generator: $p_\theta(x y = c) = p_\theta(x) = \int p_\theta(x z, y = c)p_\theta(z)dz$. However, Maximum Likelihood training is intractable again due to integral over z $\max_\theta \mathbb{E}_{p_{data}(x, y)}[\log p_\theta(x y)]$ so apply variational lower-bound once more (it is similar to before, only the input y features also).	
DCGAN: use full convolutional architecture by reshaping z into tensor, with strided convolutions for downsampling and fractional-strided convolutions for generator. LeakyReLU. LAPGAN: generate a small image and upscale to create a sharper version by feeding it to the input of the next block. We introduce multiple discriminators at different scales; start from the full resolution and downsample into the "real" image for the smaller block. Then, we can feed the upsampled blurry image as the "fake" to the discriminator and the generated to see the result. Progressive GAN: Progressively build GAN generator and discriminator from low resolution, and once trained, upsample resolution once again. StyleGAN: latent variable represents the concept of "style" as it disentangles different sources of randomness. It is concatenated with noise in the synthesis network at each resolution scale. NVAE: multiscale VAE Applications: superresolution (GAN), Image-to-image translation. Other generative models: normalizing flow, continuous time generative models, energy-based-models (NN parametrizes energy function)	
Practical implementation for solving $\min_{\theta, \phi} \max_x E_{p_{data}(x)}[\log D_\phi(x)] + E_{p_\theta(x)}[\log(1 - D_\phi(x))]$ (pseudo code): • Initialise θ, ϕ , learning rates $\gamma_\theta, \gamma_\phi$, SGD outer-/inner-loop iterations T, K • For $t = 1, \dots, T$ • # update discriminator • For $i = 1, \dots, K$ • $z_1, \dots, z_M \sim p(z)$ • $x_1, \dots, x_M \sim p_{data}(x)$ • $\phi \leftarrow \phi + \gamma_\phi \nabla_{\phi} [\frac{1}{M} \sum_{m=1}^M \log D_\phi(x_m) + \frac{1}{K} \sum_{k=1}^K \log(1 - D_\phi(G_\phi(z_k)))]$ • # update generator • $z_1, \dots, z_J \sim p(z)$ • $\hat{y}_j = G_\theta(z_j)$, $j = 1, \dots, J$ • $\theta \leftarrow \theta - \gamma_\theta \nabla_{\theta} [\frac{1}{J} \sum_{j=1}^J \log(1 - D_\phi(\hat{y}_j))]$ • # learning rates $\gamma_\theta, \gamma_\phi$ & inner-loop iterations K need to be chosen carefully! (otherwise training may be unstable)	