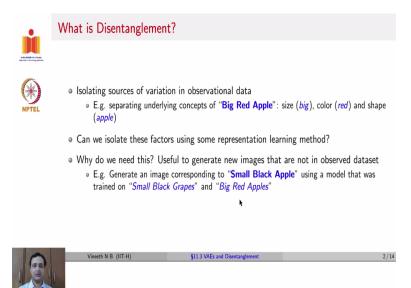
Deep Learning for Computer Vision Professor Vineeth N Balasubramanian Department of Computer Science and Engineering Indian Institute of Technology, Hyderabad Lecture 70 VAEs and Disentanglement

(Refer Slide Time: 00:14)

ete til forste som	Deep Learning for Computer Vision VAEs and Disentanglement	
NPTEL	Vineeth N Balasubramanian Department of Computer Science and Engineering Indian Institute of Technology, Hyderabad	
Cont	Vineeth N B (IIT-H) \$11.3 VAEs and Disentanglement	1/14

We have seen different variants of GANs over the last couple of lectures. We will now move on to another important notion in Generative Models, which is called Disentanglement. This notion is more closely associated with Variational Auto Encoders VAEs, and we will also discuss why this is so as part of this lecture.

(Refer Slide Time: 00:45)

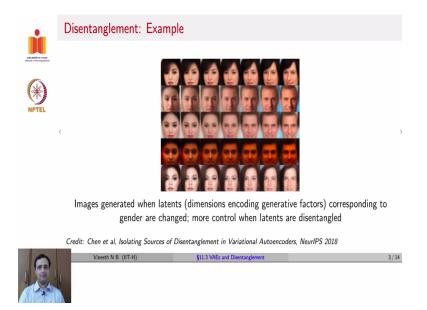


To start with, what is Disentanglement? Disentanglement is about isolating sources of variation in observational data. If you had an image of a Big Red Apple, can you separate the generative factors for such images as corresponding to size, big, color, red and shape or object apple? Can we enforce Deep Learning Models, Deep Generative Models, in particular, to isolate these factors while learning such a model? Why do we need such an approach?

If we could disentangle the generative factors, it allows us to generate new images that may not be in an observed dataset. Suppose your training dataset had images of small black grapes and big red apples. Can we generate an image corresponding to a small black apple? You may not find such an image in a real-world dataset.

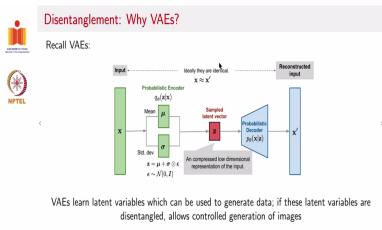
But using a deep generative model can hypothesize how this would look by setting the color to a particular value, setting the size to a particular value and the object to a particular value. You would be able to do this reliably only if the latent variables in your generative model isolate these components of images.

(Refer Slide Time: 02:32)



Here is an example of face images. In this case, the latent variables could correspond to gender, age, hair, and perhaps race so on and so forth. So if we knew which latent variable corresponded to gender, one could manipulate that latent variable alone to generate different images of different variations going from, say, female to the male gender, as you can see in the example here.

(Refer Slide Time: 03:12)



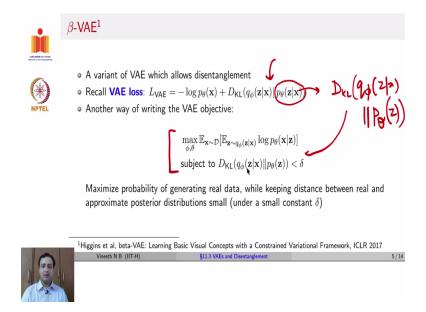


Why Variational Auto Encoders? You perhaps know the reason already. We probably already used the word latent multiple times. In GANs, generative adversarial networks, the latents are not learned per se. The latent vector is a noise from a Gaussian. In a Variational Auto Encoder, the latent variables are learned. If one could now ensure that those latent variables are disentangled, you may have a lot of control over what kind of images you can generate out of the VAE. So recall the VAE overall architecture and formulation.

So you have your input data x, the encoder provides the mean and variance of an approximate posterior, which over learning tries to become close to a pre-assumed prior. Then a vector is sampled from the prior. The decoder reconstructs the data from that sample vector. These latent variables could be a vector of multiple dimensions. If they are disentangled, you can generate more control data.

VAE-GAN frameworks, such as Adversarial Auto Encoders, can benefit from disentangling this latent variable in a VAE.

(Refer Slide Time: 04:56)



The first work that brought this notion to the community's attention and developed a method to allow disentanglement was β -VAE. Their work was published in ICLR 2017. It is primarily a variant of VAE itself. Let us see what kind of a variant. If you recall the variational autoencoder

loss, there are two terms in your evidence lower bound, one term which minimizes the negative log-likelihood.

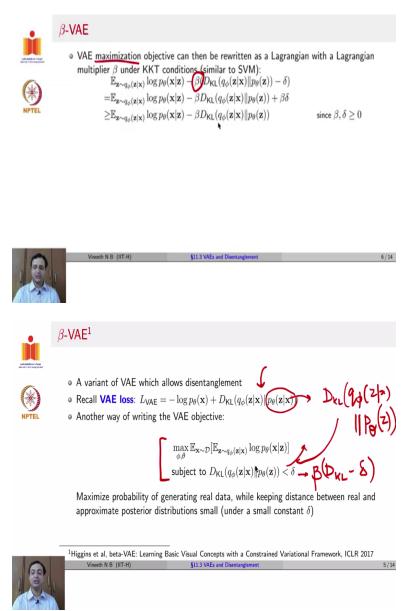
In other words, it maximizes the log-likelihood of generating that kind of data that is in the training set. The second part minimizes the KL-divergence between the approximate posterior and the true posterior. It breaks down into two terms which we finally use while training the VAE.

We finally use only the KL divergence between $q_{\phi}(z \mid x)$ and the prior $p_{\theta}(z)$ after applying the evidence lower bound. This is the correct KL to start. But this gets simplified to the KL that is written on the right side.

Now, this entire objective can be written in a slightly different manner. We can say that we would like to maximize the log-likelihood of generating x from z. Subject to the constraint that the approximate posterior q_{ϕ} and $p_{\theta}(z)$, the prior on z. The KL divergence between these two quantities is as small as possible. We say that the KL divergence should be less than some positive constant delta.

This is another way of writing out the same objective. You can say now that we are maximizing the probability of generating the real data while keeping the distance between real and approximate posterior distributions small, which boils down using the evidence lower bound to keeping the distance between the approximate posterior and the prior small. How does this help?

(Refer Slide Time: 07:52)



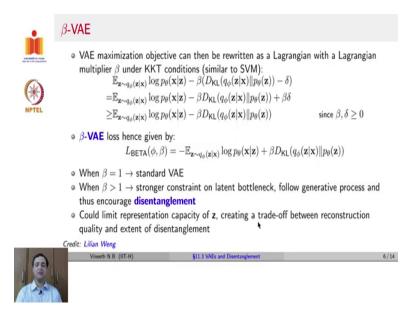
Now, keeping this optimization problem in mind, we can write it as a Lagrangian. With the Lagrangian multiplier using the KKT conditions. This is very similar to how one would write out the support vector machine objective. So this would turn out to be maximizing the log-likelihood and minimizing the constraint term that we had. This constraint term, when we have a Lagrangian, would turn out to be $D_{\kappa I} - \delta$.

And that would then go to the numerator, and you would have a Lagrangian multiplier β , using the standard Lagrangian approach to optimization. So here, we write the first term as it is the

objective function minus β , which is the Lagrangian multiplier into the constraint, which is KL-divergence between approximate posterior and prior minus δ . If you expand this, the first term stays as it is, the second term becomes minus β into the KL. When we say KL, we mean KL-divergence plus $\beta * \delta$.

Since both β and δ are quantities that are greater than or equal to 0, that is how we define them. So you are left with saying that this quantity will be greater than or equal to the log-likelihood minus the KL-divergence. We are writing this is as a maximization problem. When we do minimization, the sign will change.

(Refer Slide Time: 09:37)



One can now write the β -VAE loss to minimize, minus log-likelihood, or negative log-likelihood plus beta times the KL-divergence between approximate posterior and prior. It almost seems like nothing changed from a standard VAE which is partly true. In this case, when β is equal to 1, you would have the standard VAE. However, when β is made greater than 1, it introduces stronger disentanglement in the generative model. Why is the so?

Between these two terms used to train a VAE, the first term recall, the goal is to improve the reconstruction capability of the decoder. It is the second term that tries to learn the latents of the variational autoencoder. So by giving it a stronger weight, we are trying to make the latents be

learned better in a more disentangled way. The only problem now is this could limit the representation capacity of *z*, thus causing reconstruction problems in the entire VAE.

β-CCVE²

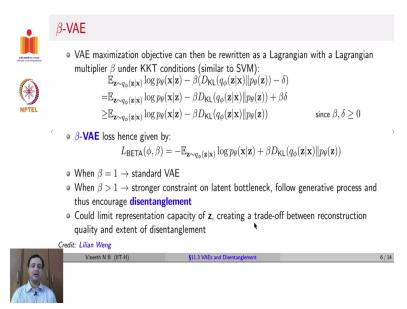
 φ-cove

 φ-cove
 <

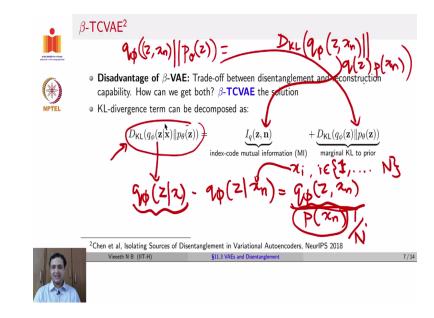
That brings us to another question which almost looks like a tradeoff between disentanglement and reconstruction capability. By increasing β in a β -VAE, we get better disentanglement, but the training procedure now thinks that the second term is more important.

(Refer Slide Time: 11:28)

(Refer Slide Time: 11:05)



In this case, the second term is more important and the first term is slightly less important. So, if the first term is slightly less important, this leads to lesser reconstruction performance.



(Refer Slide Time: 11:49)

So to address this issue, to be able to get good reconstruction and good disentanglement, there was another method introduced in NeurIPS 2018 by Chen et al., β -TCVAE. Let us try to understand this time. So the β -TCVAE looks at the KL-divergence term between the approximate posterior and prior and then decomposes it into two parts. How is this decomposition done? This decomposition is done by looking at the term, the approximate posterior $q_{\phi}(z \mid x)$, which could also be written as $q_{\phi}(z \mid x_n)$.

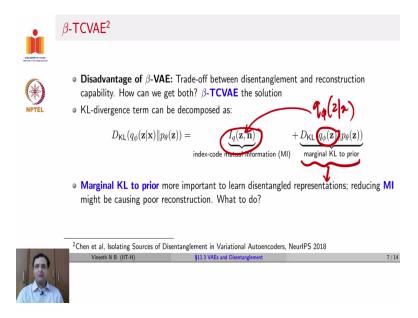
Now assume that you have a set of data points going from, say 1 to N, and each x_i is one data point where *i* comes from 1 to N. So that is the x_i that we are talking about is each of the data points. This is the same just expansion of writing the approximate posterior. So by standard probability, we can now write this as the joint probability, $q_{\phi}(z, x_n)$ by the probability on x_n , $p(x_n)$. Assuming all data points are equally likely, the denominator here would be 1/N, which is a constant.

So, you could now say that we could replace the approximate posterior with the joint probability between the latent and each data point x_n . This means that the KL-divergence between the

approximate posterior and the prior can be broken down into two parts. It can also be written as KL between $q_{\Phi}(z, x_n)$, the joint, with respect to the prior on z. The first term here, q_{Φ} can be broken down into two parts.

The first term would be the KL-divergence between the marginal on z with respect to the approximate prior, and the second term would be a KL-divergence between the joint distribution $q_{\phi}(z, x_n)$ and the product of the marginals $q(z) * p(x_n)$. This is given by the mutual information between z and n; n denotes the indices of the data points on x. Note that mutual information is defined as a constant factor of a KL-divergence between the joint distribution between two random variables and the product of its marginals. Now how does this decomposition help?

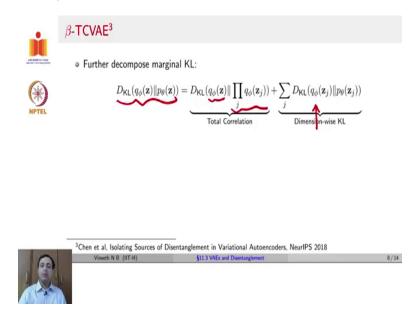
(Refer Slide Time: 15:13)



Once we have this decomposition, one notice is that the second term is the marginal KL; we will call that marginal KL because the approximate posterior has now been marginalized. Earlier, we had $q_{\phi}(z \mid x)$, but that got marginalized. The other term now came into the mutual information. This marginal KL is the component responsible for disentanglement.

Hence, trying to penalize the mutual information may lead to poorer reconstruction. Keeping this in mind, we now want to ensure that we focus on the marginal KL while learning a VAE; that is the term that we want to weigh with a beta.

(Refer Slide Time: 16:08)

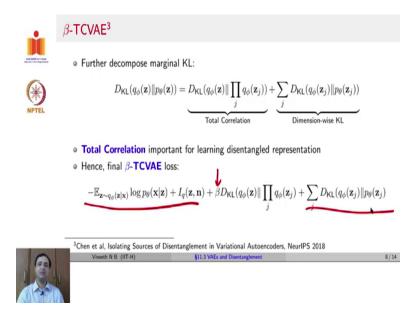


Before we do that, we will do one more thing: decompose the marginal KL divergence even further. The marginal KL divergence can be decomposed into a term that looks at the KL divergence between z, the random variable, and the product of the marginals of each dimension of z. This term is known as Total Correlation. Although the name is a misnomer, Total Correlation is a concept from Information Theory which is a generalization of mutual information to multiple random variables.

If you add two random variables z and n that we saw on the previous slide, you look at the joint and the product of the marginals of the two random variables and take the KL divergence. In total correlation, we do this for all the random variables involved in z in this particular context. Those random variables for us are the different dimensions of the z. The second term here is the dimension-wise KL-divergence and the sum of all of them.

So we have broken the overall KL divergence of z into dimension-wise quantities. Why is that important? Because in disentanglement, we would like each dimension to have a unique existence.

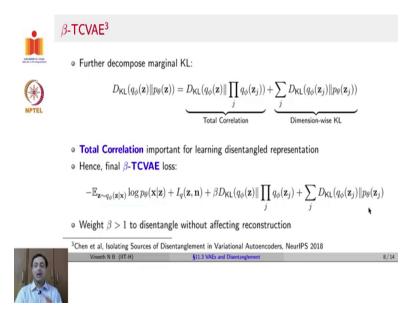
(Refer Slide Time: 17:45)



Now, suppose you look at this decomposition. In that case, one notices that total correlation is perhaps most important for disentangled representations. That term is responsible for looking at each dimension of z to the overall z. This leads us to the final loss for the β -TCVAE, which simply puts together all the components that we have seen so far, the negative log-likelihood, the mutual information, the total correlation, and the dimension-wise KL, which are the different components we have seen.

What is different? Notice, β is only on total correlation and not on any other terms in the overall objective.

(Refer Slide Time: 18:36)



This allows us to focus β on disentanglement only on that term and not affect the reconstruction capabilities of the VAE.

(Refer Slide Time: 18:47)

•	Disentangled Representation Learning: How to evaluate?
ededalihi inconsen de sato discolgi ginitati	Mutual Information Gap (MIG)
()€)	\circ Use mutual information between generative factors (g) and latent dimensions (z) in some way; how?
NPTEL	\circ Compute mutual information between each generative factors $({\bf g}_i)$ and each latent dimension $({\bf z}_i)$
	\circ For each \mathbf{g}_i , take $\mathbf{z}_j, \mathbf{z}_l$ that have highest and second highest mutual information with \mathbf{g}_i
	• $MIG = \frac{1}{K} \sum_{i=1}^{K} \frac{1}{H(\mathbf{g}_i)} (I(\mathbf{g}_i, \mathbf{z}_j) - I(\mathbf{g}_i, \mathbf{z}_l))$ where $H(\mathbf{g}_i)$ is entropy of \mathbf{g}_i and $0 \le I(\mathbf{g}_i, \mathbf{z}_j) \le H(\mathbf{g}_i)$
	$\circ~$ Averaging by K and normalizing by $H(\mathbf{g}_i)$ provides values between 0 and 1
	$\circ~MIG \to 0$: bad disentanglement, $MIG \to 1$: good disentanglement
	• Why not simply use MI? Why MI gap? Homework! (Hint: Read metric section in Chen et al, Isolating Sources of Disentanglement in Variational Autoencoders, NeurIPS 2018)
1	Vineeth N B (IIT-H) §11.3 VAEs and Disentanglement 9/14

Having seen β -VAE and β -TCVAE, one question that arises now is how do you evaluate whether your generative model has learned to disentangle effectively? While one way is to generate different images and check qualitatively whether those images represent different generative factors, that can become a tedious exercise for many generative factors. One such metric that has been proposed in recent years is known as the Mutual information Gap (MIG). The idea is to use the mutual information between generative factors, g and latent dimensions, z in some way.

What do we mean by generative factors? These are factors that we know exist in the dataset. If we say, big red apple, size, color, and object represent the generative factors. The idea is to see if the latent dimensions z that are learned capture these generative factors somehow. We would like to use the mutual information between the random variables g and the latent dimensions z to capture this.

How do we do this? We compute the mutual information between each generator factor, g_i and each latent dimension, z_i . You would then have an entire matrix of mutual information between every pair, g_1 and z_1 , g_1 and z_2 , g_2 and z_1 , so on and so forth. What do we do with all of these mutual information values? For each generator factor g_i consider the latent factors that have the top two mutual information values. Let us call them z_i and z_i .

Once we have this, we define the mutual information gap as the difference in the mutual information values between these top two latent factors. So, the mutual information of g_i with z_j and g_i with z_i , will be the mutual information gap with some normalization factor on the outside. What is the normalization factor? $1/H(g_i)$, the entropy of g_i intrinsically, i.e., entropy is

 $-\sum p \ logp$ of that generative factor.

And this normalization takes care of averaging this across all of the generative factors. So averaging by K and normalizing by H, entropy, provides us values between 0 and 1. If the mutual information gap is zero, both these latent factors have high mutual information with the same generative factor. It would be considered a bad disentanglement because both those latents are learning the same thing. They are not disentangled.

On the other hand, when MIG is 1, it is good disentanglement. One question here is why do we use the mutual information gap and not just mutual information itself? Think about it. It is

homework for you. If you need to understand this better, read the paper "Isolating Sources of Disentanglement", NeurIPS 2018 paper, which defined this metric.

(Refer Slide Time: 23:06)

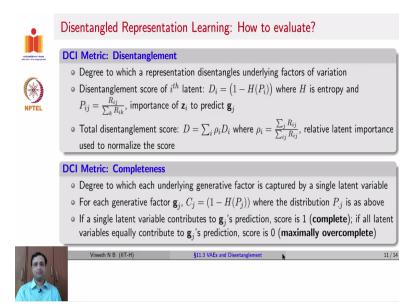
	Disentangled Representation Learning: How to evaluate?
webscheihlitzurs tenan allen auszt diezwispiejstecht	
()	DCI Metric ^a
	^a Eastwood and Williams, A Framework for the Quantitative Evaluation of Disentangled Representations, ICLR 2018
NPTEL	\circ Considers three properties of representations: D - Disentanglement, C - Completeness, I - Informativeness
	• Train a model (e.g. β -VAE) to get latent representations
	• Get latent representation of each image in a dataset
	• Train k linear regressors (one for each \mathbf{g}_i), $f_1 \dots f_k$, to predict \mathbf{g}_i given z
	$ullet$ From the regressors, we get W_{ij} (how much $oldsymbol{z}_i$ is important to predict $oldsymbol{g}_j$)
	• Create a relative importance matrix R such that $R_{ij} = W_{ij} $
	Vineeth N B (IIT-H) §11.3 VAEs and Disentanglement 10/1

Another metric for checking disentanglement that has been recently proposed in ICLR 2018 is known as the DCI Metric. DCI stands for Disentanglement, Completeness and Informativeness. There is a quantity defined for each of these. To compute them, let us first train any model, say Beta-VAE, to learn latent representations. Get the latent representation of each image in a training dataset or the test dataset, for that matter, if that is where you would like to study for disentanglement.

Then we train a linear regressor. So you learn k different linear regressors, f_1 f_k , that predicts each generative factor g_i given the entire latent vector z. So you have k different generative factors, and hence k different linear regressors. How do you learn them? For each input image, you would get a latent factor z, and you want to use that now to predict the gender here? Or what was the color of this Apple?

That would be the value of each generative factor. Once we train these linear regressors, it will give you a weighted combination of each latent factor. That is what linear regression does. So you would now have an entire matrix, W_{ij} , which tells us how much a latent factor z_i is important to predict a generative factor g_j . We will call this the relative importance matrix, which is the absolute value of W_{ij} 's, obtained through regressors.

(Refer Slide Time: 25:10)



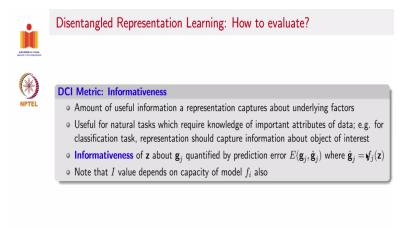
Once we get the relative importance matrix, there are quantities defined for disentanglement: completeness and informativeness. Let us look at disentanglement first. This metric tries to capture the degree to which representation disentangles underlying factors of variation. This is obtained by defining D_i as $1 - H(P_i)$, where H is the entropy of P_i . What is the probability distribution P_i ? P_i is defined as a vector of P_{ij} 's for each generator factor g_j , where each P_{ij} is given by R_{ij} in that matrix divided by all the entries in that particular row *i* corresponding to that latent factor.

So, that is the disentanglement score of the *i*th latent. So, we ideally want the latent to predict only one generative factor and not predict all. So, the Total Disentanglement score is then given by summation $\rho_i D_i$, where D_i was the disentanglement score of only the *i*th latent. So, the overall disentanglement score is given by summation $\rho_i D_i$, where the coefficient ρ_i is given by summation over *j*, R_{ij} divided by summation over *ij*, R_{ij} , which is the normalization over the column of that importance matrix.

The second metric is completeness, which is the degree to which a single latent variable captures each underlying generative factor. For each generative factor g_{i} , the completeness is defined as

 $1 - H(P_j)$, where P_j is defined as above. If a single latent variable contributes to g_j 's prediction, the score would be 1. We only want one latent variable to correspond to a generative factor. If all latent variables contribute equally to g_j 's prediction, the score is 0 because that represents the opposite of disentanglement. We call that situation maximally over complete, where all latent factors correspond to just one generative factor in the data.

(Refer Slide Time: 28:00)





The third metric is Informativeness. How informative are the disentangled latent representations? This measures how useful, a representation is in capturing the underlying factors. This is considered with respect to a specific task. For example, a classification task in which you would like the latent representation to capture information about the object of interest. How do we measure this?

The prediction error gives the Informativeness of z about a particular generator factor g_j between the original generator factor and the predicted generator factor. It is obtained using one of those regressors that we had defined earlier. These metrics, including informativeness, depend on the goodness of those regressors that we use in the first step.

(Refer Slide Time: 29:11)

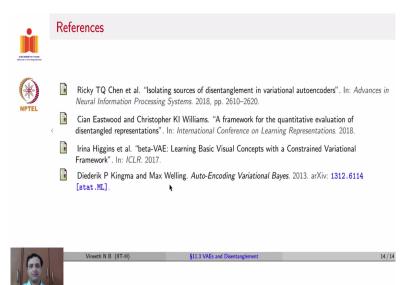




That completes our discussion of disentanglement. I hope it provided you with an introduction to the topic, a couple of methods that enforce disentanglement, as well as how to measure whether a generative model is disentangled. As homework, please read this excellent blog, *"From Autoencoders to Beta-VAE"*. Another blog on *"Review of Disentanglement with VAEs"* and optionally, the papers that we referred to in the slides.

We left behind the question in the first mutual information gap metric: *Why the gap and not just mutual information itself*? Think about it and we will discuss it next time.

(Refer Slide Time: 30:00)



References.