



# Specialist Programme on Artificial Intelligence for IT & ITES Industry

Al Applications: Process & Best Practice

Dr Barry Shepherd barryshepherd@nus.edu.sg

Singapore e-Government Leadership Centre National University of Singapore

© 2020 NUS. The contents contained in this document may not be reproduced in any form or by any means, without the written permission of ISS, NUS other than for the purpose for which it has been supplied.

Transform

Inspire

Lead

# **Agenda**



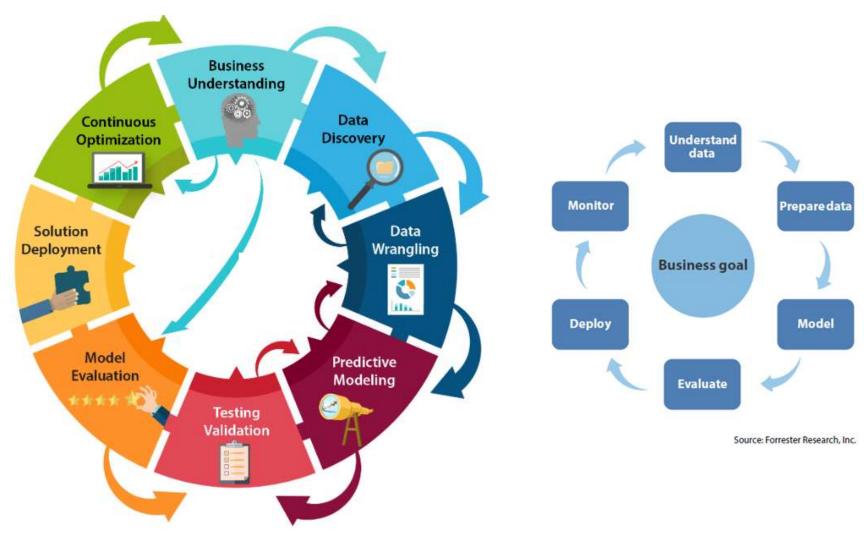
- Al Applications
- Process and Best Practices



Challenges & Issues







**Predictive Analytical Model Process Flow** 

# **Setting Business Goals**



- Usually a two way process between the Data Scientists / Al experts and the domain experts
  - The Data Scientist / All expert usually needs **some** domain knowledge for this conversation to succeed



- Business Goal Guidelines
  - Use only business terms make no mention of analytics methods!
  - There must be an actionable outcome
  - Must be able to measure success (quantifiable metrics)



### **Setting Business Goals / Metrics**

Possible examples are ...

■ Improve the response rate for a direct marketing campaign by 50%

■ Increase the average order size by 2 items

Determine what drives customer acquisition identify top 2 factors

■ Forecast the size of the customer base in the future 80% accuracy on test set?

■ Retain profitable customers reduce churn of top 20% customers by 10%

Recommend the next, best product for existing customers get 20% buy rate lift?

■ Choose the right message for the right groups of customers too vague?

By how much?

Need clear success criteria





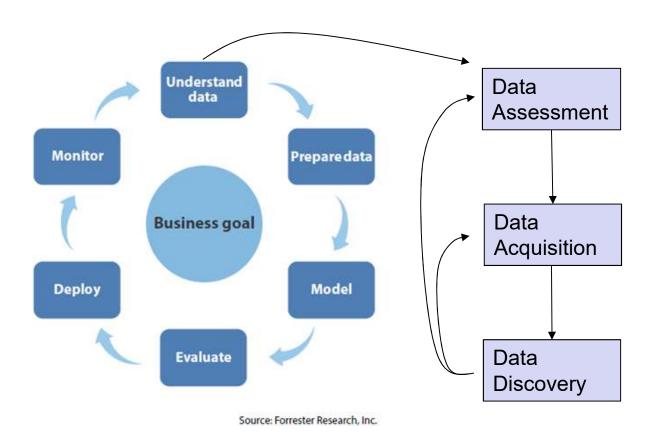
#### **Business Goals are not Technical Goals**

- A business goal states objectives in business terminology
  - E.g. "Increase sales to existing customers."
- A technical goal states project objectives in technical terms.
  - E.g. "Predict how many widgets a customer will buy, given their purchases over the past three years, demographic information (age, salary, city, etc.), and the price of the item."





# **Model Building Process**



Assess what data you have and what you need to start to collect / acquire

Basic analysis & visualisation to gain insights





# **Identifying Data Requirements**

- Questions to Answer:
  - What data is available?
  - What must the data contain?
  - What would be useful? (whether available or not ) innovate!
  - What is the right level of granularity?
  - What volume of data is needed?
  - How much history is required? how far back in time should the data go?
- What data is required for comparison?
  - What is currently being done?
    - E.g. what is the existing churn rate, response rate, failure rate?
  - Obtain a control group ~ data describing the status quo
    - E.g. what happened to patients who did not receive the treatment?
    - E.g. what did customers buy who did not see the ad?







- Consolidate all of your data requirements
- Determine what (if any) essential data is missing
- How to bridge the gap?
  - Put in place mechanisms to start collecting the missing data (delay the analytics)
  - Get the data from elsewhere (e.g. 3<sup>rd</sup> party, the web)
  - Innovate to obtain missing data or data you think may be useful

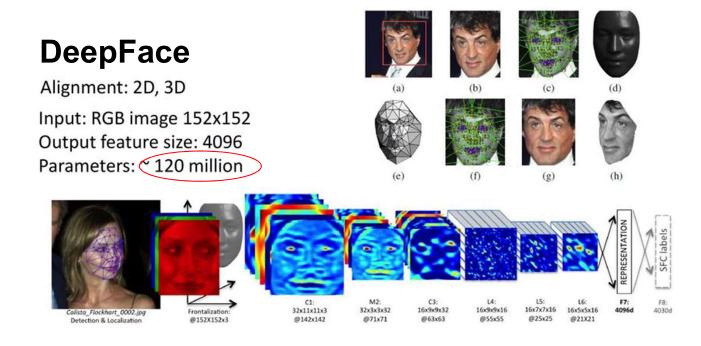






# Do I have Enough Data?

- How much data is required for Machine Learning / Deep Learning?
- Simple answer = LOTS
- Common rule of thumb is 10 examples per model parameter (e.g. per NN weight)



Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. Deepface: Closing the gap to human-level performance in face verification. In CVPR, 2014





# **Data Augmentation - Images**

- **rotation**: random with angle between 0° and 360° (uniform)
- translation: random with shift between -10 and 10 pixels (uniform)
- rescaling: random with scale factor between 1/1.6 and 1.6 (log-uniform)
- flipping: yes or no (bernoulli)
- shearing: random with angle between -20° and 20° (uniform)
- stretching: random with stretch factor between 1/1.3 and 1.3 (log-uniform)

Classifying plankton with deep neural networks
MARCH 17, 2015

https://benanne.github.io/2015/03/17/plankton.html



Gaussian noise and cropping are two common methods

Many python libraries exist for image augmentation, e.g. imgaug (over 60 methods), see

https://towardsdatascience.com/data-augmentation-for-deep-learning-4fe21d1a4eb9





# **Data Augmentation - Business Data?**

- Required for Data Balancing (e.g. when one class is very rare)
- Adding noise
- Creating duplications
- Synthesising "similar" cases (e.g. SMOTE)
- Using statistical distributions to generate simulated data (harder)

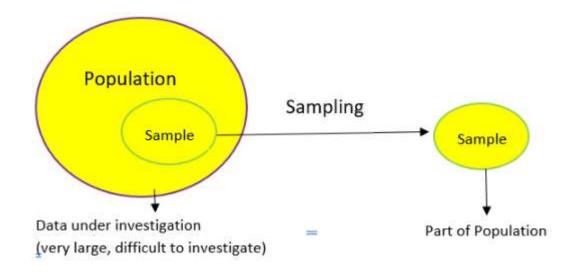


#### **Too Much Data?**

Many Big Data proponents say use it all....

"Collecting large amount of data & then processing it to make Inferences from them involves different costs associated with it"

Raw "big data" is often very noisy, low signal-to-noise ratio



E.g. randomly select 10% of records

but what if the training signal is very rare? – use stratified sampling or similar





- Predictive Models typically use Supervised Learning
  - The training dataset must contain examples of all of the decision classes
  - This can often be a challenge: tedious & time-consuming

#### Al Platform Data Labeling Service

Al Platform Data Labeling Service lets you work with human labelers to generate highly accurate labels for a collection of data that you can use in machine learning models.

Labeling your training data is the first step in the machine learning development cycle. To train a machine learning model, provide representative data samples that you want to classify or analyze, along with the machine learning algorithm to handle each sample. For example, to train a model that can identify flowers in images, you must label objects like sunflowers, roses, and tulips in the image dataset. To train a model that can identify the names of diseases in medical documents, you must highlight disease-related words in the document dataset.

To start data labeling in Al Platform Data Labeling Service, create three resources for the human labelers:

- A dataset containing the representative data samples to label
- . A label set listing all possible labels in the dataset
- · A set of instructions guiding human labelers through labeling tasks

Once you've created these resources, you submit them as part of a labeling request. The human labelers start annotating the items in the dataset according to your instructions. After human labelers finish the labeling, you can export well labeled datasets and use the datasets in the machine learning development.

# Get someone else to do it

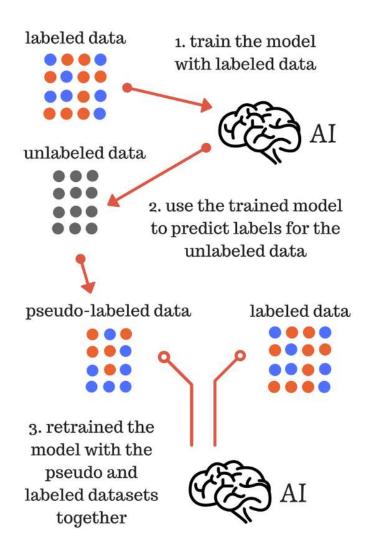
(e.g. get your students to do it!)



Google Cloud AI & Machine Learning Products

# **Avoiding the Data Labelling chore**





#### Pseudo Labelling

- One form of Semi-Supervised Learning
- Good for if you have a small amount of labelled data and lots of unlabelled

Can do iteratively, e.g.

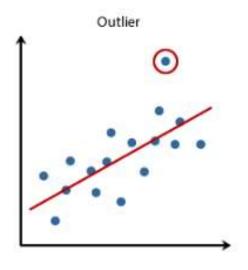
- Add only the most confident predicted labels into the training data
- Build new model
- o repeat



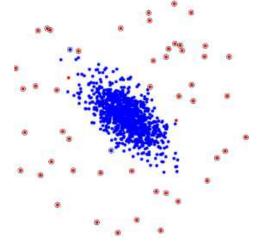


# **Avoiding the Data Labelling chore**

- Unsupervised Learning build a model to "describe" the data
  - Good if the target pattern is relatively rare, e.g. people without disease, machines with no faults, people who don't buy....
  - Identify the minority class as outliers those that don't fit the usual situation
  - If labels are available then model only the baseline (normal) situation,



E.g. Fit lines or curves to the baseline data, look at distance to the best fit line or curve

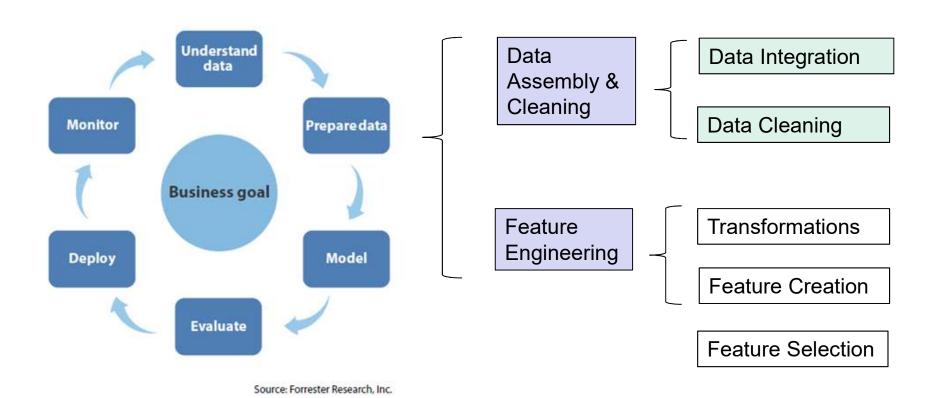


E.g. Cluster the baseline data, anything far away from the cluster centres is an outlier





# **Predictive Modeling Process**



OC-EGBGL-AI/Alprocess-and-bestpractice/VI.3

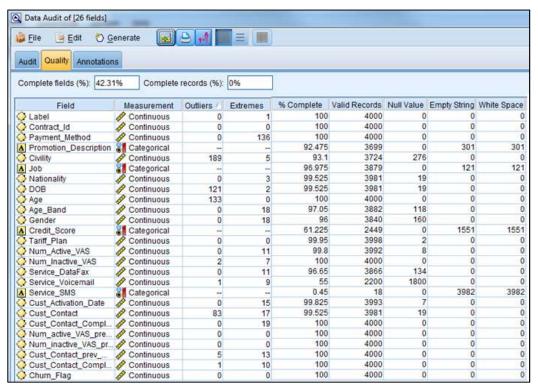




#### **Data Audit**

A useful starting point is the **Data Audit.** 

- Is the data adequate?
- Is it what you expect?, Does it look sensible?
- What are the data quality issues?



Data Audit Tool from SPSS Modeller





# **Data Cleaning**



- Handle missing values
- Handle noisy / erroneous data
- Handle outliers
- Correct inconsistent data
- Resolve redundancy caused by data integration









# Handling Missing Values

- Data Imputation fill in the missing values automatically
  - Guiding Principle: Avoid adding bias and distortion to the data
  - Understand why the data is missing can help guide the imputation
  - Often a missing value means zero or the default value. E.g. for 'rainfall' variable, a missing value may mean no rain on that day  $\rightarrow 0$

#### Common Options

- A global **constant** : e.g., "unknown" or 0 (zero)

Easy, but modeling algorithms may mistakingly treat "unknown" as a concept

- The **attribute mean** (or median, mode)
  - Simple and quick though not always satisfactory
- The **attribute mean** for all samples belonging to the **same class**

Often a better estimate than attribute mean

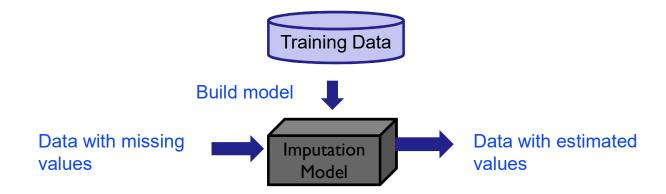
Gender	Children	Salary	Bought PEP
М	I	29,000	Y
М	0	65,000	Y
F	2	-	Y
М	0	47,000	Y
F	-	15,000	N
-	I	23,000	N
F	Ī	36,000	N





# **Data Imputation**

- Train a prediction model (e.g. regression model, decision tree) to predict the most probable value
  - Use variables containing values to estimate the variable with missing values
  - Can produce good estimates.
  - Need training data and additional modeling







#### **Outliers**

- Observations that "deviate so much from other observations as to arouse suspicion that it was generated by a different mechanism". (Hawkins, 1980)
- Appearing at the maximum or minimum end of a variable, skewing or distorting the distribution
  - E.g. extreme weather conditions on a particular day, a very wealthy person financially very different from the rest of the population, etc.



Outliers may be errors (remove)

or

they may be valid data (keep, or handle another way)

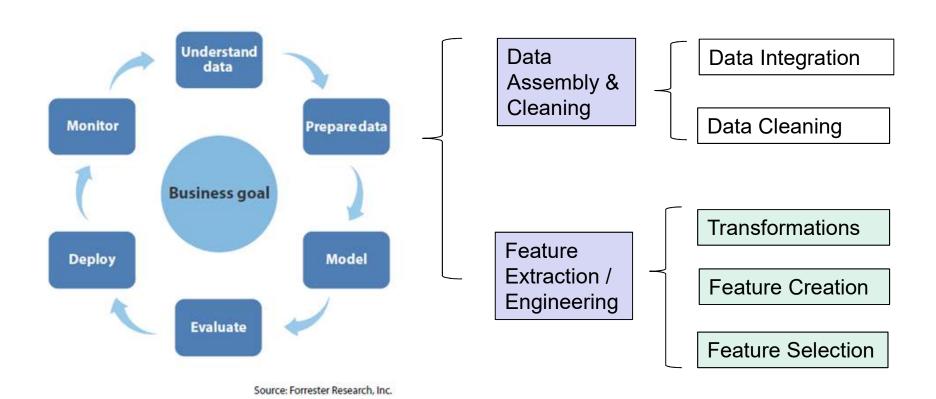
#### **Identifying Outliers**

- Statistical tests for variance
- Clustering
- Human inspection





# **Predictive Modeling Process**

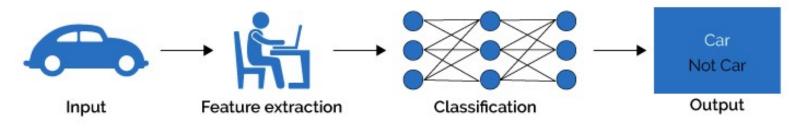




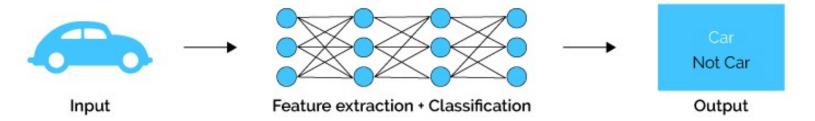


# Feature Engineering for DL?

#### Machine Learning



#### Deep Learning



# Data Transformations - Normalisation



- Reduces outlier distortion and enhances linear predictability
- Ensure all variables have approximately the same scale
  - E.g. variable Age vs Income: a distance of 10 "years" may be more significant than a distance of \$1000, yet \$1000 swamps 10 numerically
- Common Methods....

$$v' = \frac{v - min_A}{max_A - min_A}$$

$$v' = \frac{v - min_A}{max_A - min_A} \qquad v' = \frac{v - mean_A}{stand\_dev_A} \qquad v' = \frac{v}{10^j} \qquad \text{Where } j \text{ is the smallest integer such that } Max(|v'|) < 1}$$

$$v' = \frac{v}{10^{i}}$$

Min-max scaling

Z-score scaling

Decimal scaling



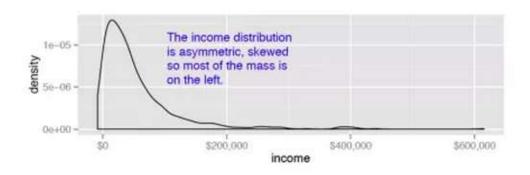
zero mean unit variance (ZMUV) normalization

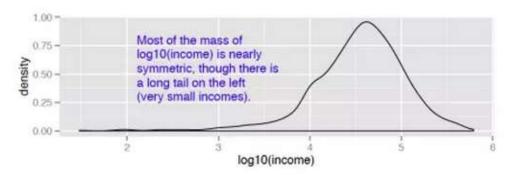
For images this will normalise over different brightness and contrast ranges

# **Data Transformations - Logs**



- Makes a skewed attribute more symmetric
- Reduces the magnitudes
- Common bases 10, 2, e (which base to use is often not important)





- Incomes, customer value, account or purchase sizes—are commonly encountered sources of skewed distributions in data science applications.
- Often they are log-normally distributed: the log of the data is normally distributed





# **Transforming Categorical Data**

- How to handle...
  - Marital status = single, married, divorced, widowed?
- Could convert to a single new integer variable...
  - Marital status = 0,1,2,3 where
     0 = single, I=married, 2=divorced, 3=widowed

**Integer Encoding** 

- Better to create four new T/F variables
  - $\circ$  Single = 0, I
  - $\circ$  Married = 0, I
  - Divorced = 0, I
  - Widowed = 0, I

**One-Hot Encoding** 







#### **Feature Construction**

Deriving a value that is more useful / making something more explicit, e.g.

<u>ID</u>	Cost per unit	Units purchased
1.	10	10
2.	15	5
3.	8	8
4.	10	5



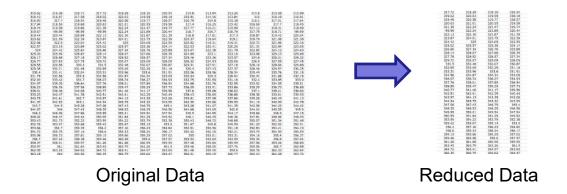
<u>ID</u>	Cost per unit	Units purchased	Total \$ Revenue
1.	10	10	100
2.	15	5	75
3.	8	8	64
4.	10	5	50





#### **Feature Construction: PCA**

- PCA = Principle Component Analysis
- Generates new features as linear combinations of the old ones
- New features are created to explain the variance most efficiently
- Often used as a mechanism to do feature reduction and/or data visualisation







# **Feature Decomposition**

■ Decomposing compound features into simpler components, e.g....

<u>ID</u>	Product Holdings	Purchased Service
1.	"ProdA, ProdC"	Y
2.	"ProdB, ProdC"	N
3.	"ProdA, ProdD"	N
4.	"ProdB, ProdD"	Y
	J	L

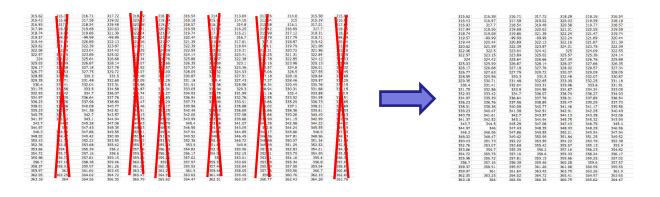
ID	ProdA	ProdB	ProdC	ProdD	Purchased Service
1.	1	0	1	0	Y
2.	0	1	1	0	N
3.	1	0	0	1	N
4.	0	1	0	1	Y

...



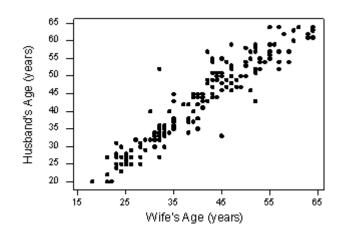


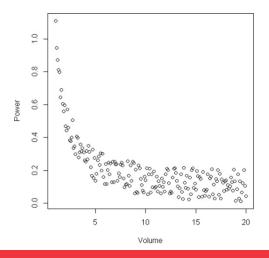
#### **Feature Selection**



Selecting the most relevant attributes

- Good input features are those that correlate with the target
  - Beware the inputs and target may be correlated non-linearly, or linear only in a certain range
  - Sometimes two inputs that have poor correlation with the target when considered alone may correlate well when combined, e.g. predicting spending power from a family income and family size





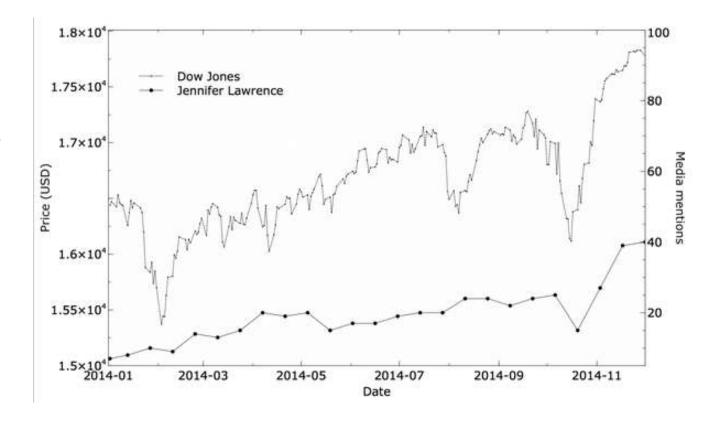




#### **Correlation vs Causation**

- Correlation does not imply causation.
  - If A and B are correlated it does not mean A causes B or vice versa
- Model inputs need not be causal factors
  - BUT there should be some plausible link with the target

Both increase over the same period (correlation = 0.86) but there is no connection! We cannot predict the Dow Jones using Jennifer Lawrence



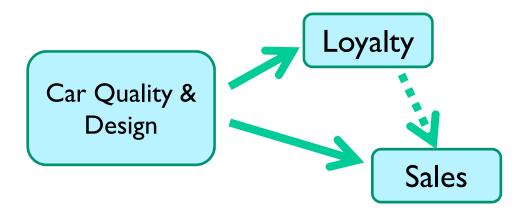




# Correlation can be good!

#### Correlation is often a result of hidden Causal Factors

Loyalty and sales may be correlated but loyalty does not (necessarily) cause sales. Instead a hidden (latent) causal factor may be at play....



...but loyalty may still be a useful predictor in the absence of suitable model input variables describing car design and car quality





#### **Correlation can be bad!**

- Input features that are highly correlated may be redundant can be omitted
- Input features that correlate with each other are not independent
  - Linear regression assumes there is no multi-collinearity between the inputs
- BUT many modelling methods can perform well even if inputs are correlated, so check the model performance using all input variables first as a *baseline* (if practical)
- Beware of leakers ~ inclusion of the target (in some disguised form) into the input variables
  - E.g. If we are predicting **Age** then we can't put **Date of Birth** as an input
  - Easy to do if you are not familiar with the problem domain and/or the variable names are not informative (e.g. "F23B")
  - CLUE: Very high correlation between an input variable and the target







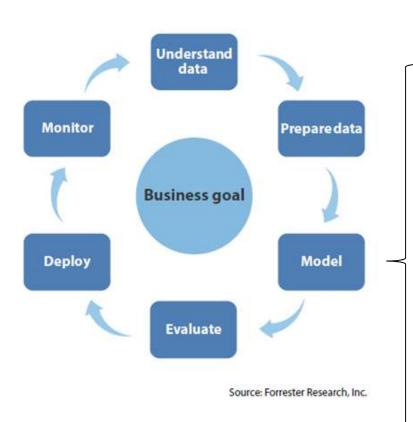
# Feature Engineering for IOT & Sensor Data

- Signal Processing cheat sheet?
- Time Series signal processing
- Contrast with tech analysis for stock data etc?
- https://www.datasciencecentral.com/profiles/blogs/training-with-historical-data-surelyyou-re-joking-says-the-iot





# **Predictive Modeling Process**



Create Model Test Plan

**Data Balancing** 

Select Model Type & Model Parameters

**Build Model** 

**Evaluate Test results** 





### Selecting Training & Test sets

In order to test the model, it is necessary to divide the data into training and test sets, e.g.

70% training  $\frac{Build\ Model}{and\ Apply\ to}$  30% test

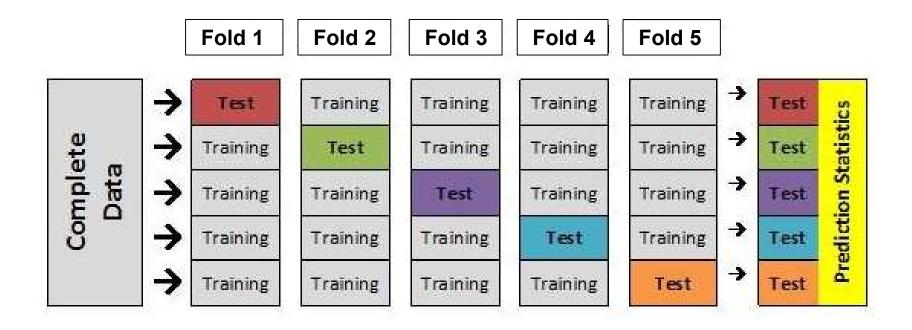
- Select the training data randomly (unless it's a time series problem).
- Usually select the test set to be everything not in the training set
- Simple split is good for large data sets





### **Selecting Training & Test Sets**

- K-fold Cross-validation
  - $\blacksquare$  Divide the data into k subsamples. Use k-l as training data and one as test data
  - Use for data set with moderate size

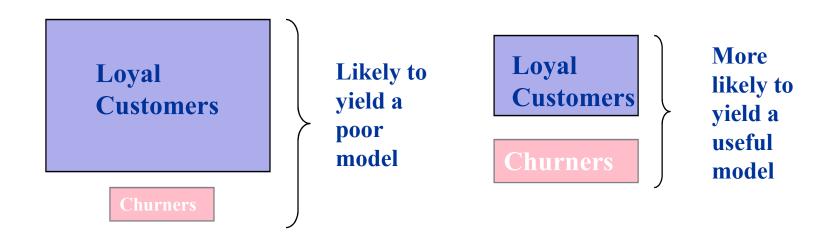






## **Data Balancing**

- Unbalanced training data can result in poor models
- E.g. 9900 records where decision = loyal100 records where decision = churner
  - The mined model is likely to be decision = loyal (99% correct!), very accurate but useless for predicting churn!
- Solution = balance the data as much as practical

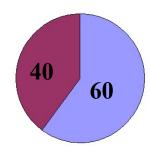






## **Data Balancing**

- It's not necessary to achieve equal size categories
  - Between 20/80 and 40/60 is OK
- Common methods use "oversampling"
  - Delete records from the most frequent category
  - Duplicate records in the less frequent category



## SMOTE (Synthetic Minority Oversampling)



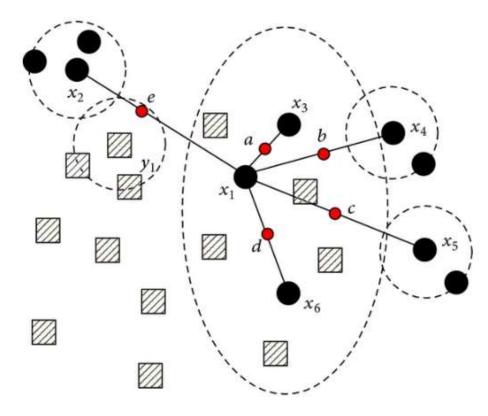


An over-sampling approach in which the minority class is over-sampled by creating ``synthetic" examples rather than by over-sampling with replacement.

#### Add new minority class instances by:

- For each minority class instance c
  - neighbours = Get KNN(5)
  - n = Random pick one from neighbours
  - Create a new minority class r instance using c's feature vector and the feature vector's difference of n and c multiplied by a random number

» i.e. r.feats = c.feats + (c.feats - n.feats) \* rand(0,1)



- Majority class samples
- Minority class samples
- Synthetic samples





#### **Classification Evaluation Metrics**

Actual \Predicted	Predicted <b>True</b>	Predicted <b>False</b>	Sum
Actual <b>True</b>	True Positives (TP)	False Negatives (FN)	Р
Actual <b>False</b>	False Positives (FP)	True Negatives (TN)	N
Sum	Ρ'	N'	

- Accuracy = (TP + TN)/AII
- Error rate: I accuracy, or
  - Error rate = (FP + FN)/All
- Sensitivity: True Positive Rate
  - Sensitivity = TP/P
- Specificity: True Negative Rate
  - Specificity = TN/N

- Precision: what % of predictions are correct?
  - Precision = TP/P'
- Recall: what % of actual responders were predicted?
  - Recall = TP/P





#### The Confusion Matrix - Model A

Be sure to use the right metric for the business problem at hand

	Predicted buyer	Predicted Non-buyer	Total
Actual Buyer	200 True Positives	100 False Negatives	300
Actual Non-Buyer	800	1900	2700
	False Positives	True Negatives	
Total	1000	2000	3000

This model gets 70% correct (2100/3000, overall accuracy) but only 66% of the actual buyers (200/300) are captured by the model.





#### The Confusion Matrix - Model B

- Test results for a second model
- Is this a better model than the previous one?

	Predicted buyer	Predicted Non-buyer	Total
Actual Buyer	280	20	300
	True Positives	False Negatives	
Actual Non-Buyer	1000	1700	2700
	False Positives	True Negatives	
Total	1280	1720	3000

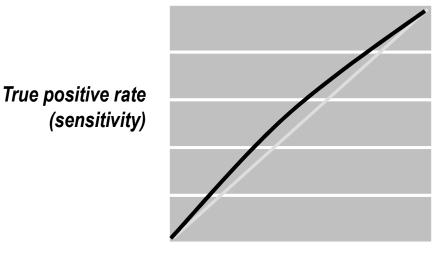
This model gets only 66% correct (1980/3000) but 93.3% of the actual buyers (280/300) are captured by the model.

# Model Assessment with ROC Chart NUS National University of Singapore



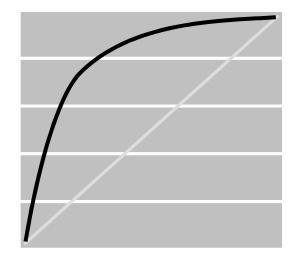


#### weak model



False positive fraction (1-specificity)

#### strong model



False positive fraction (1-specificity)

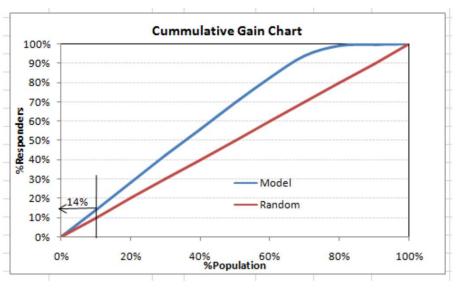
(sensitivity)





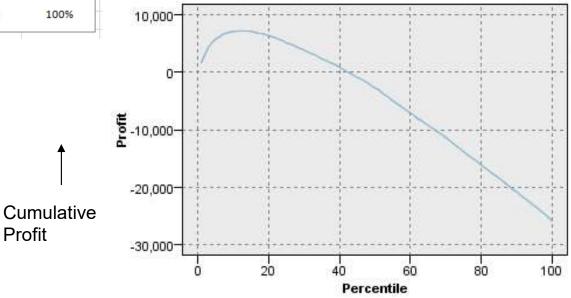
#### **Model Assessment with Gains Chart**

**Profit** 



In many situations a cumulative profit (or ROI) chart can add more insight:

E.g. If you know the cost of sending a mailing and the revenue obtained when a positive response occurs







#### **Comparison with Baselines**

- The accuracy required by a model can only be determined by examining the (business) context in which it will be used
- E.g. For ad click models,
  - Overall display ad CTR is 0.05%, rich media ad CTR is 0.1%, and Facebook Ad CTR ranges from 0.5% to 1.6%. Non-targeted CTR ~ 0.05% (Doubleclick, 2018)
- Compare Model results against a Baseline model
  - E.g. what was the accuracy if random guessing was used?
- Compare Model results against a quick First-Try model

## Always start with a stupid model, no exceptions.

How to efficiently build Machine Learning powered products.





Fundamentally, a baseline is a model that is both simple to set up and has a reasonable chance of providing decent results. Experimenting with them is usually quick and low cost

A baseline will take you less than 1/10th of the time, and could provide up to 90% of the results

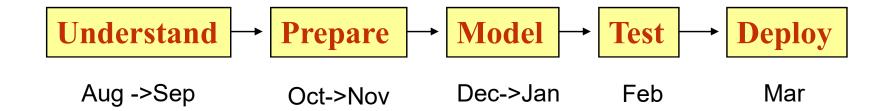
https://blog.insightdatascience.com/always-start-with-a-stupid-model-no-exceptions-3a22314b9aaa





### Overall Execution: Incorporating Agile

Its not linear pass through the various stages....



Instead... Try to work in short iterations. Each iteration generates a prototype working system which is tested and then refined and improved over time – using test results and feedback from stakeholders

Caution: Data Preparation can often occupy the majority of the project time — often up to 80%!





#### **Being Agile – Frequent iterations**

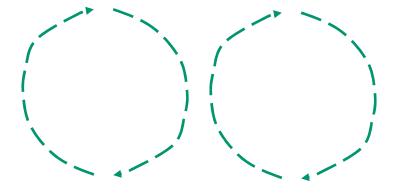
**Increasing Business Understanding ->** 

**Increasing Data Preparation ->** 

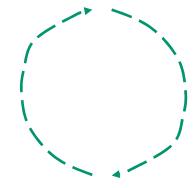
**Improving Models ->** 

**Lab Testing ->** 

**Production Testing ->** 





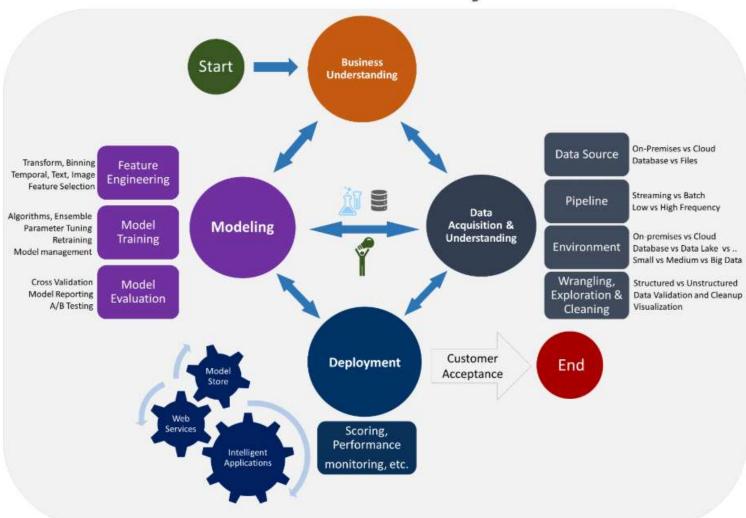






## Microsoft TDSP (Team Data Science Process)

#### **Data Science Lifecycle**



https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/overview





### From DevOps to MLOps

Developing and deploying ML systems can be relatively fast and cheap, but maintaining them over time is often difficult and expensive.







## ML Lifecycle Management Issues (e.g.'s)

#### Entanglement

\* Changing Anything Changes Everything (CACE). Applies to input signals, hyper-parameters, learning settings, sampling methods, convergence thresholds, data selection etc

#### Correction Cascades

- A model m1 for a problem may exist, but a model for a slightly different problem is needed
- $\clubsuit$  A fast solution is to learn a model m2 that takes m1 as input and learns a small correction
- $\clubsuit$  But this creates a system dependency on m1, making it expensive to change m1 in future
- \* The cost increases when correction models are cascaded

#### Undeclared Consumers

- $\diamond$  Often, a prediction from a model m1 is made widely accessible, either at runtime or by writing to files or logs that may later be consumed by other systems.
- \* Without access controls, some of these consumers may be undeclared, silently using *m1* output as an input to another system.
- Changes to m1 will very likely impact these other parts, potentially in ways that are unintended, poorly understood, and detrimental. Undeclared consumers may also create hidden feedback loops

https://papers.nips.cc/paper/5656-hidden-technical-debt-in-machine-learning-systems.pdf