AI Sharing

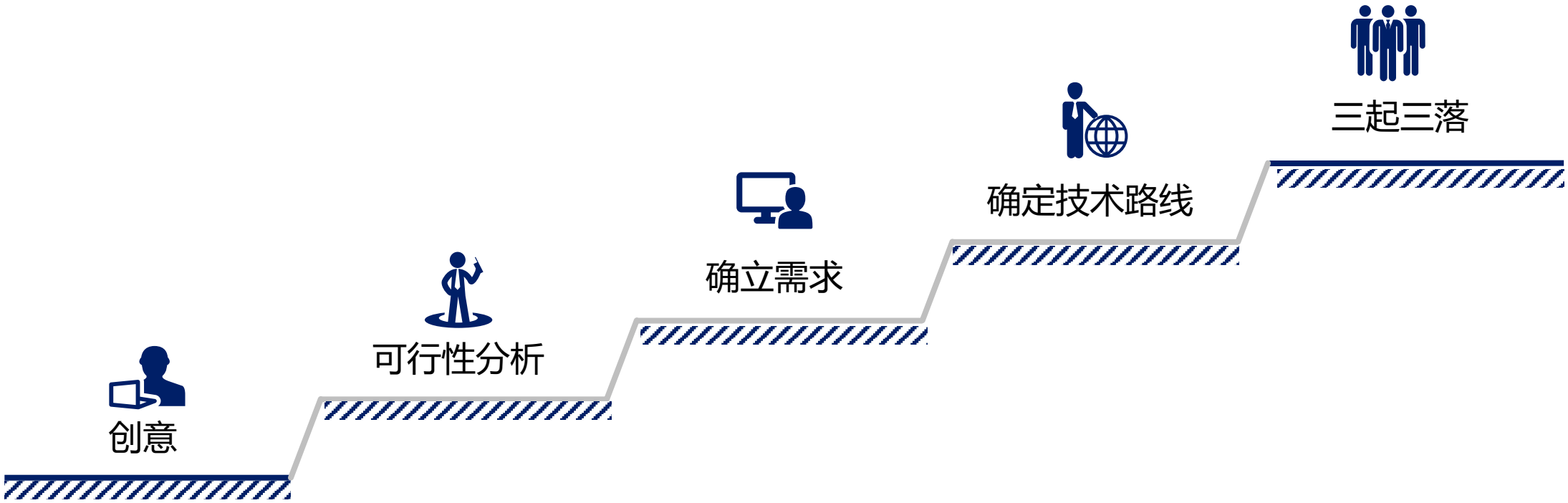
Jim Xie

2021/7/20

大纲

1. 起源与发展
2. 案例分析一（机器学习）
3. 案例分析二（深度学习）
4. 趋势Projects
5. 安全领域热点

起源与发展



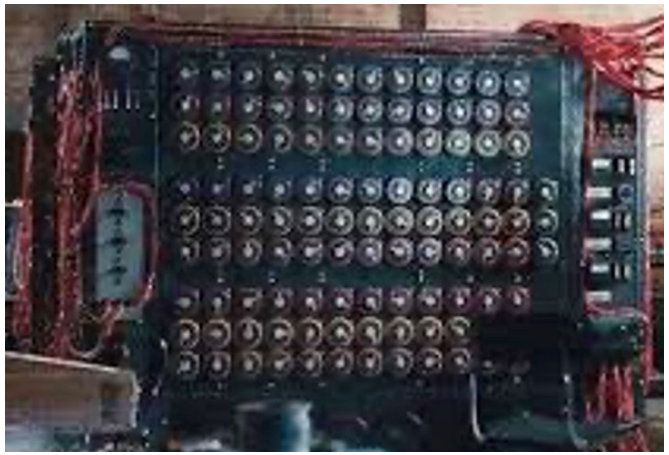
创意

上世纪三，四十年代

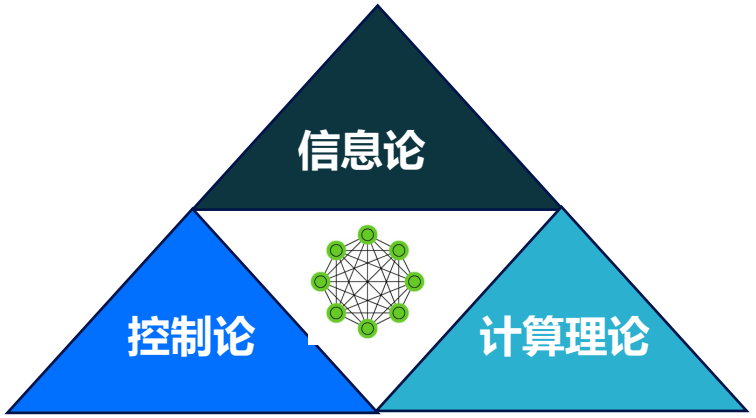
神经元活动

人造大脑

可行性

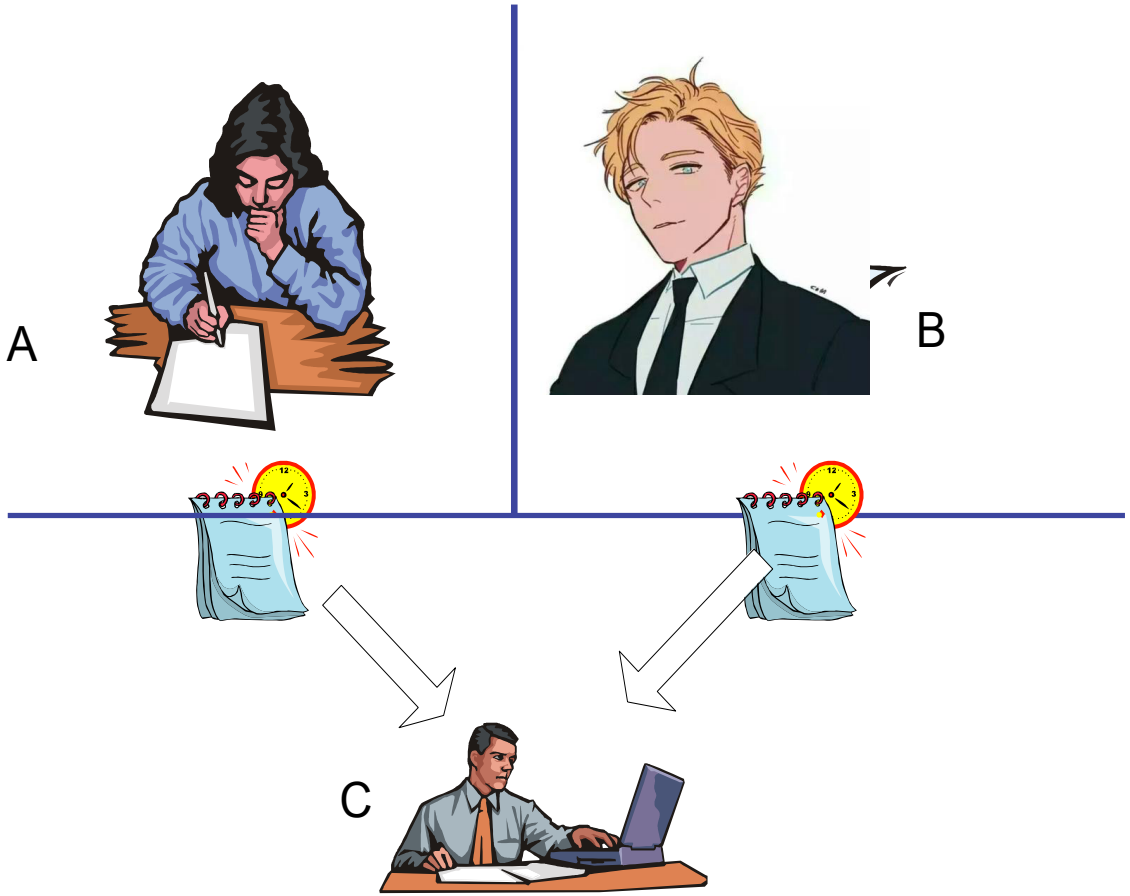


1. 如何通过机械状态表示信息？
2. 如何组织状态，信息如何流动？
3. 通过状态机进行运算？



1+3

明确需求



- 绕开智能的定义
- 定义了测量标准

路径选择：符号主义

John MacCarthy

又称为逻辑主义，认为智能源于逻辑，知识可以通过符号进行表达和演变，推理过程即为符号操作变换的过程，可以通过计算机将人类的知识表达出来并加以转换，从而实现人工智能。

代表应用：搜索引擎/专家库

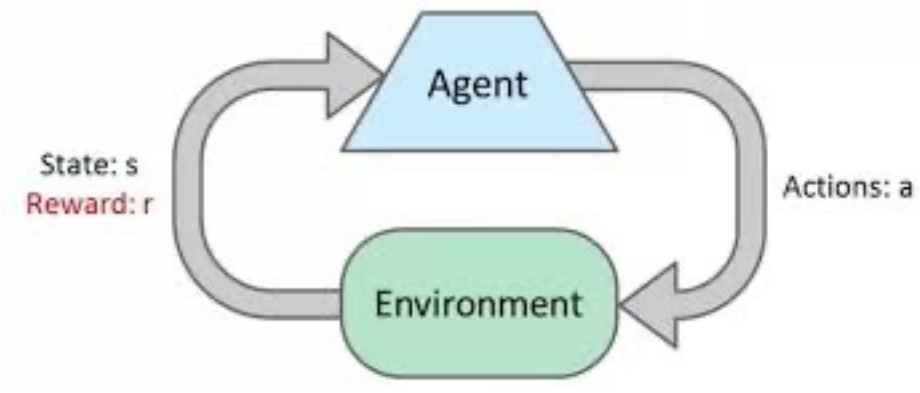
路径选择：连接主义

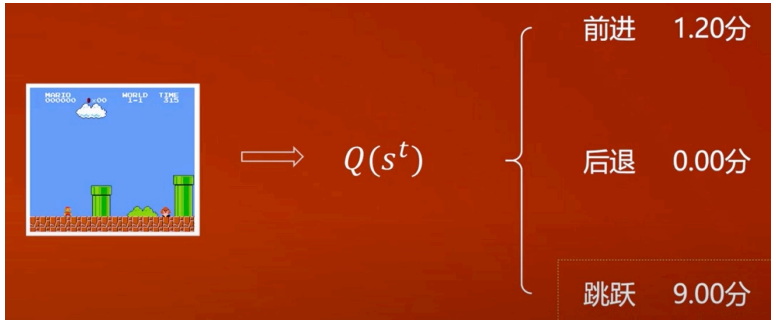
Marvin Minsky

认为智能源于仿生学，特别是对人脑的模拟，通过对人脑结构的模拟可以产生智能。

代表应用：神经网络/深度学习

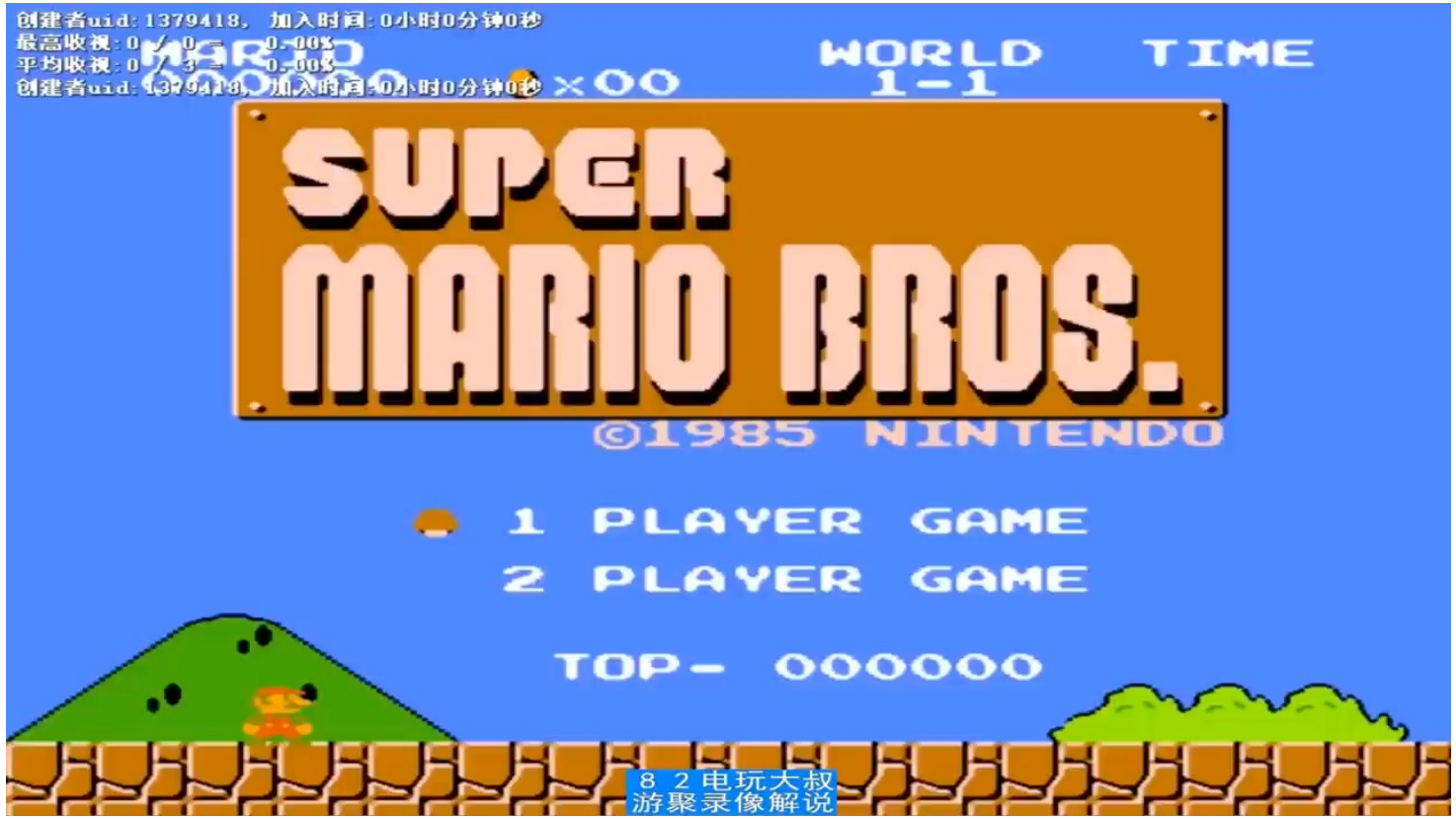
路径选择：行为主义





代表应用：Alpha Zero

行为主义


创建者uid:1379418, 加入时间:0小时0分钟0秒
最高收视:0 / 0 = 0.00%
平均收视:0 / 3 = 0.00%
创建者uid:1379418, 加入时间:0小时0分钟0秒
MARIO
000000
×00
WORLD
1-1
TIME
SUPER
MARIO BROS.
©1985 NINTENDO
1 PLAYER GAME
2 PLAYER GAME
TOP- 000000
8 2电玩大叔
游聚录像解说

三起三落

1956 — 诞生

达特茅斯会议
逻辑主义
连接主义
行为主义
感知机模型
….

1974 — 进入低谷期

公众期望过高
DARPA停止拨款
异或问题
….

1980 — 崛起

专家系统
神经网络模型
异或问题被解决
….

1987 — 进入低谷期

计算机算力瓶颈
通用计算机崛起
专家系统市场崩溃
….

1993 — 重新崛起

深蓝在比赛中获胜
深度学习领域突破
AlphaGo战胜人类
….

至今 — 热潮?

机器学习：找规律

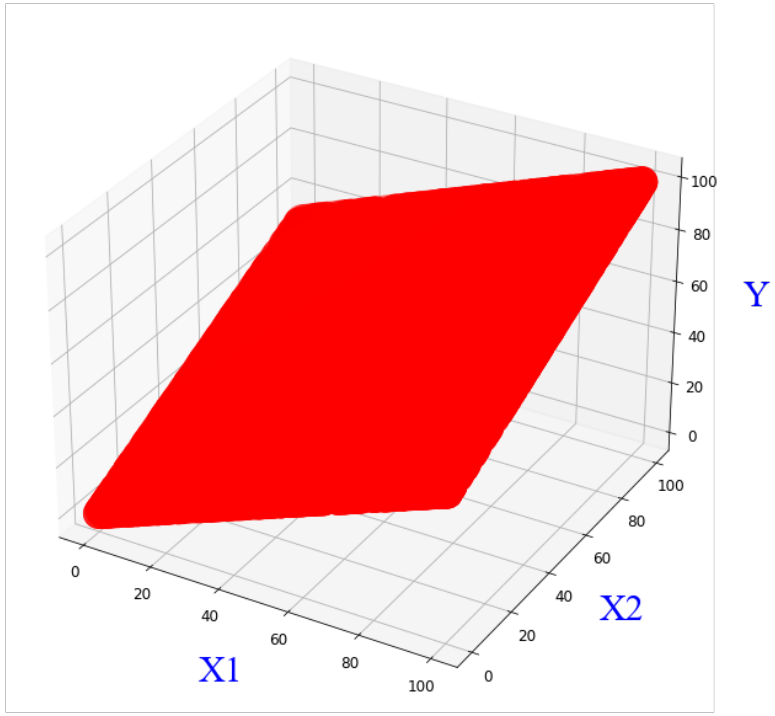
How

X_1	X_2	Y
18	63	40. 5
8	87	47. 5
38	95	66. 5
48	44	46. 0
67	4	35. 5
90	76	83. 0
19	21	20. 0
76	25	50. 5

$$Y = \frac{X_1 + X_2}{2}$$

如何找规律？

1 **定范式**　2 定损耗　3 做优化



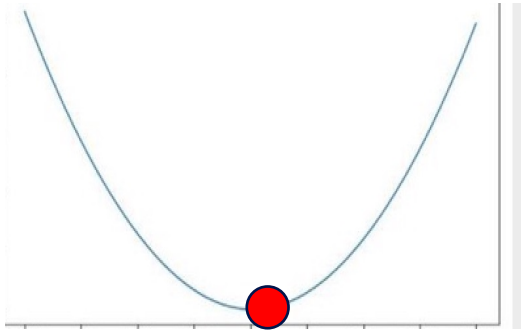
$$y = k_1x_1 + k_2x_2 + b$$

$$\begin{bmatrix} k_1 \\ k_2 \\ b \end{bmatrix} = \ ?$$

如何找规律？

1 定范式　　**2 定损耗**　　3 做优化

$$J=\frac{1}{2}\sum\left(Y-(k_1*x_1+k_2x_2+b)\right)^2$$

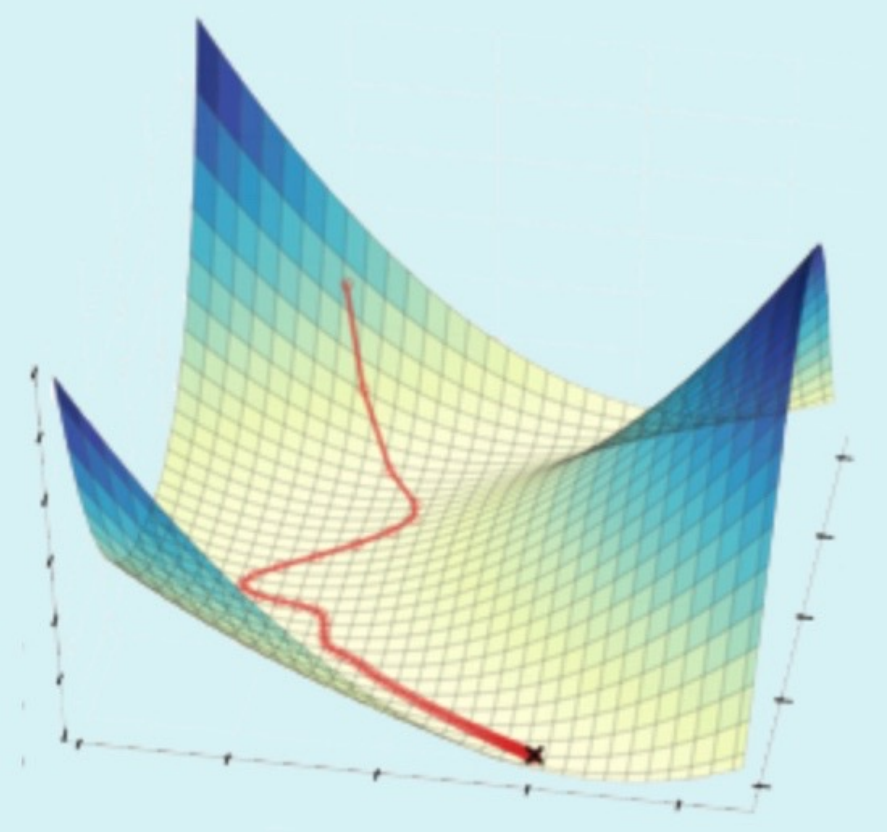


$$\begin{cases}\dfrac{\partial J}{\partial k_1}=0\\ \dfrac{\partial J}{\partial k_2}=0\\ \dfrac{\partial J}{\partial b}=0\end{cases}$$

如何找规律？

1 定范式　2 定损耗　3 **做优化**

模型和算法区别



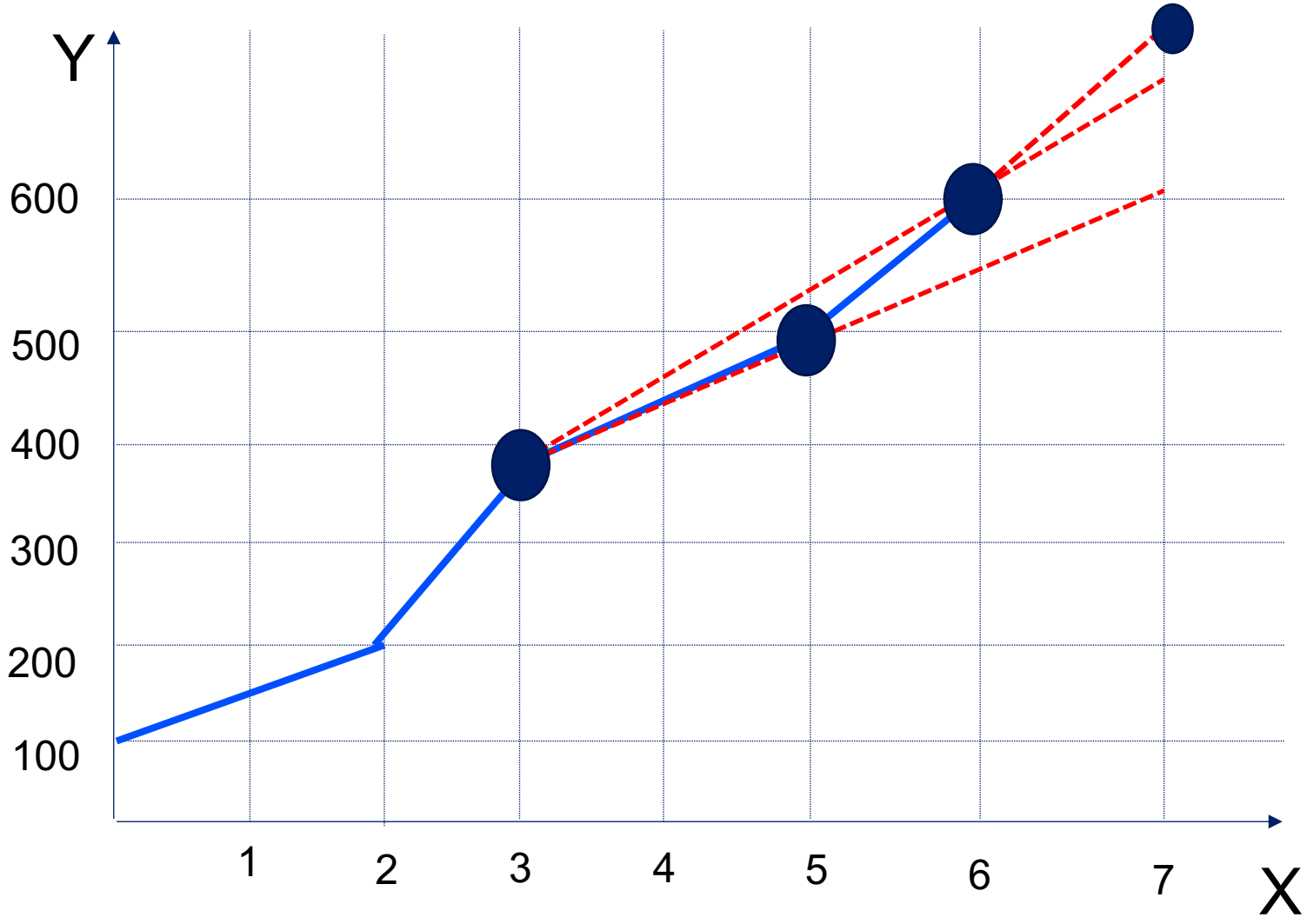
案例一：销售预测

代理商	客户名称	产品序列号	注册日期
nqb0k	_DYNAbit Test	CE50E_FQXA-FMPK-BFFB	2021/7/1
xtvoe	Akinola Ltd	CE50E_NDCR-FMPK-BFFB	2021/7/1
r7j4z	CE Test FR	CE50E_NDCA-FMPK-BFFB	2021/7/1
ckdtm	CE Test Ireland	CE50E_BKPA-FMPK-BFFB	2021/7/1
edbbw	CE Test UK	CE50E_QNZZ-FMPK-BFFB	2021/7/3
vgzoa	CE_Test	CE70E_RQFA-FMBX-BFFB	2021/7/3
ulqyu	CE50 Test Baltics	CE50E_YFCZ-FMPK-BFFB	2021/7/1
h0ahb	CE50 Test EE	CE50E_YYXZ-FMPK-BFFB	2021/7/1
mqkqg	CE50 Test IT	CE50E_KKRM-FMPK-BFFB	2021/7/1
y1193	CE50 Test Poland	CE50E_DWMR-FMPK-BFFB	2021/7/5
oczkj	CE50 Test Switzerland03	CE50E_BBXZ-FMPK-BFFB	2021/7/1
cski4	cebulk202005251151	CE50E_HETB-OP5T-U6PO	2021/7/1
cski4	cebulk202005251151	CE50E_33JJ-BZ2P-CZWY	2021/7/18
cski4	cebulk202005251424	CE50E_Q27Q-MTBS-M96L	2021/7/19

原始数据

7/1	55001
7/2	55104
7/3	55114
	…
7/18	56001
7/19	56205
7/20	?
7/21	?

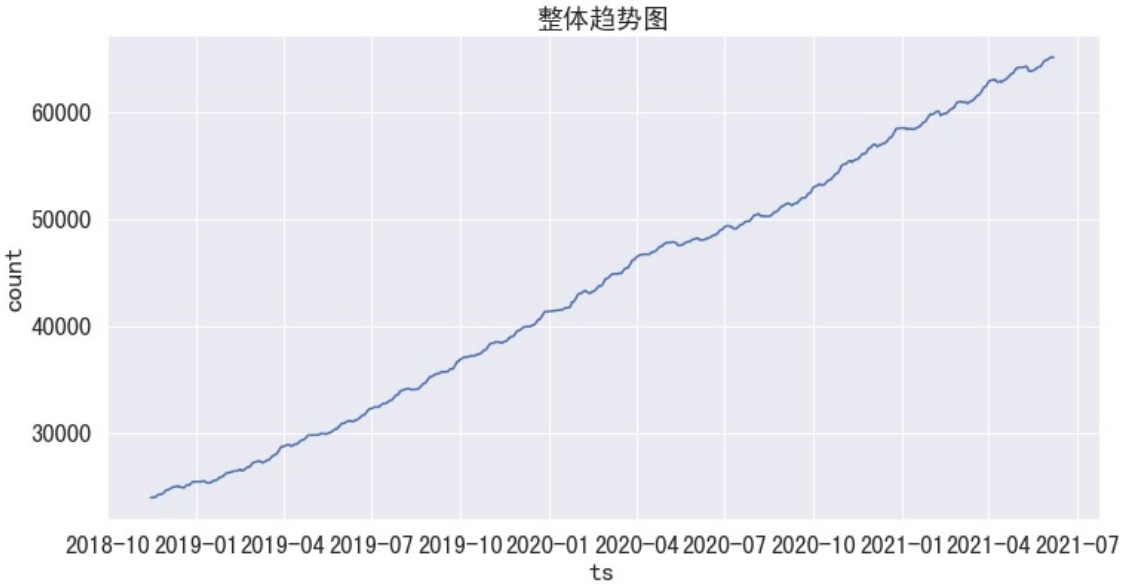
时序预测原理

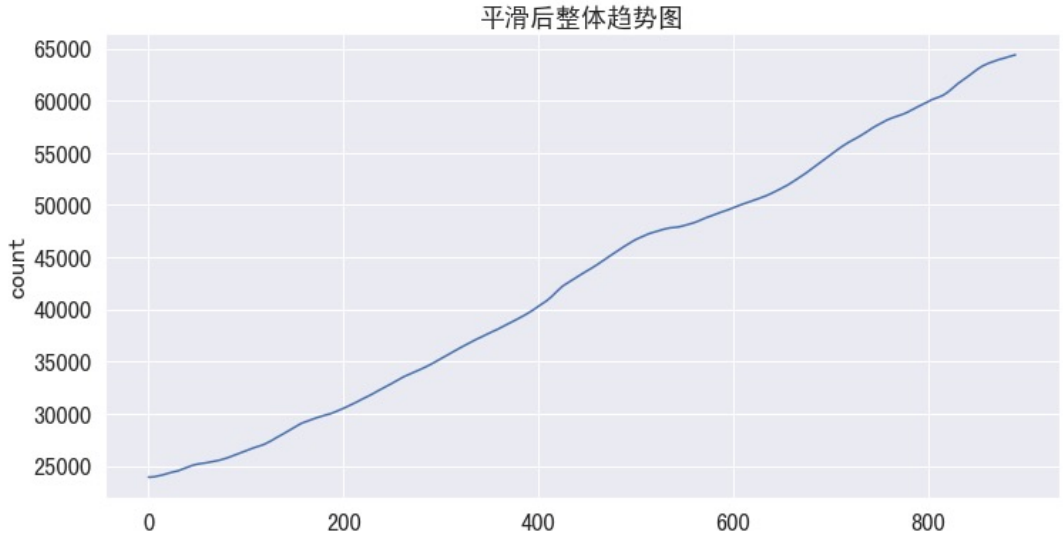


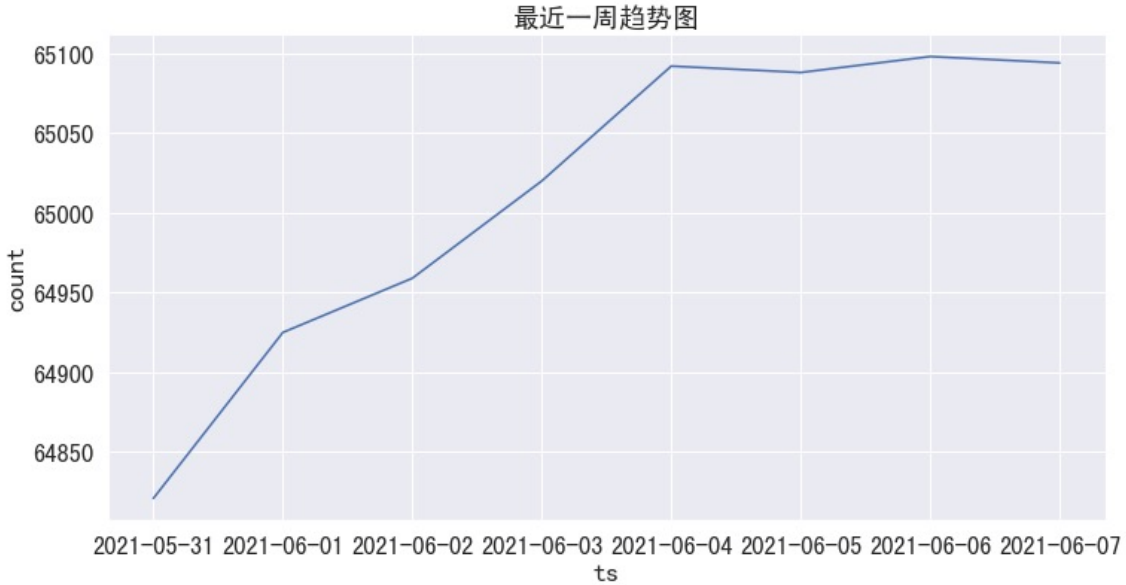
当X=7 时， Y等于几比较合适？

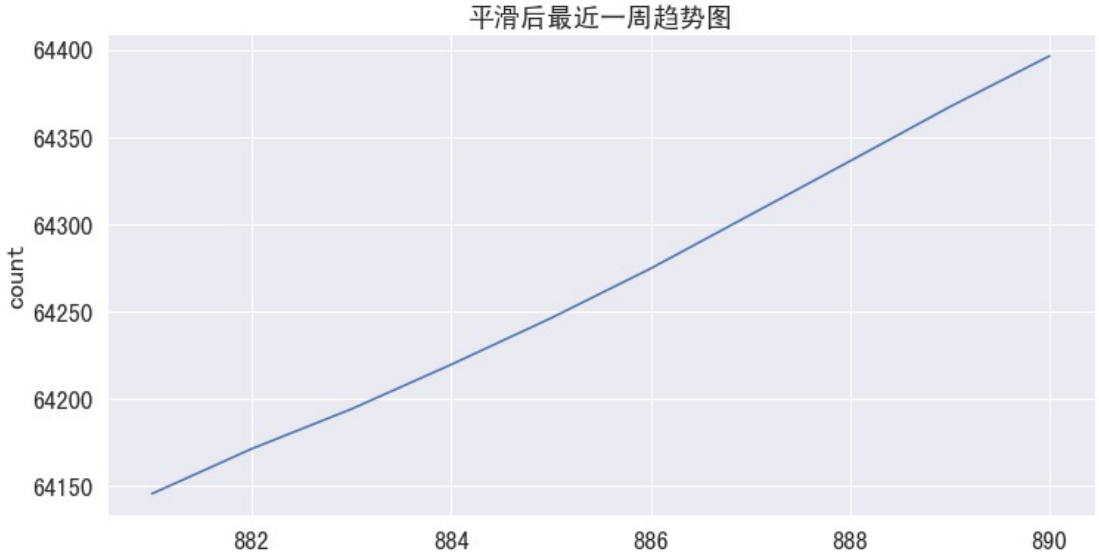
$$y = k_0x_0 + k_1x_1 + k_2x_2 + k_3x_3 \cdots$$

解题：先看走势图

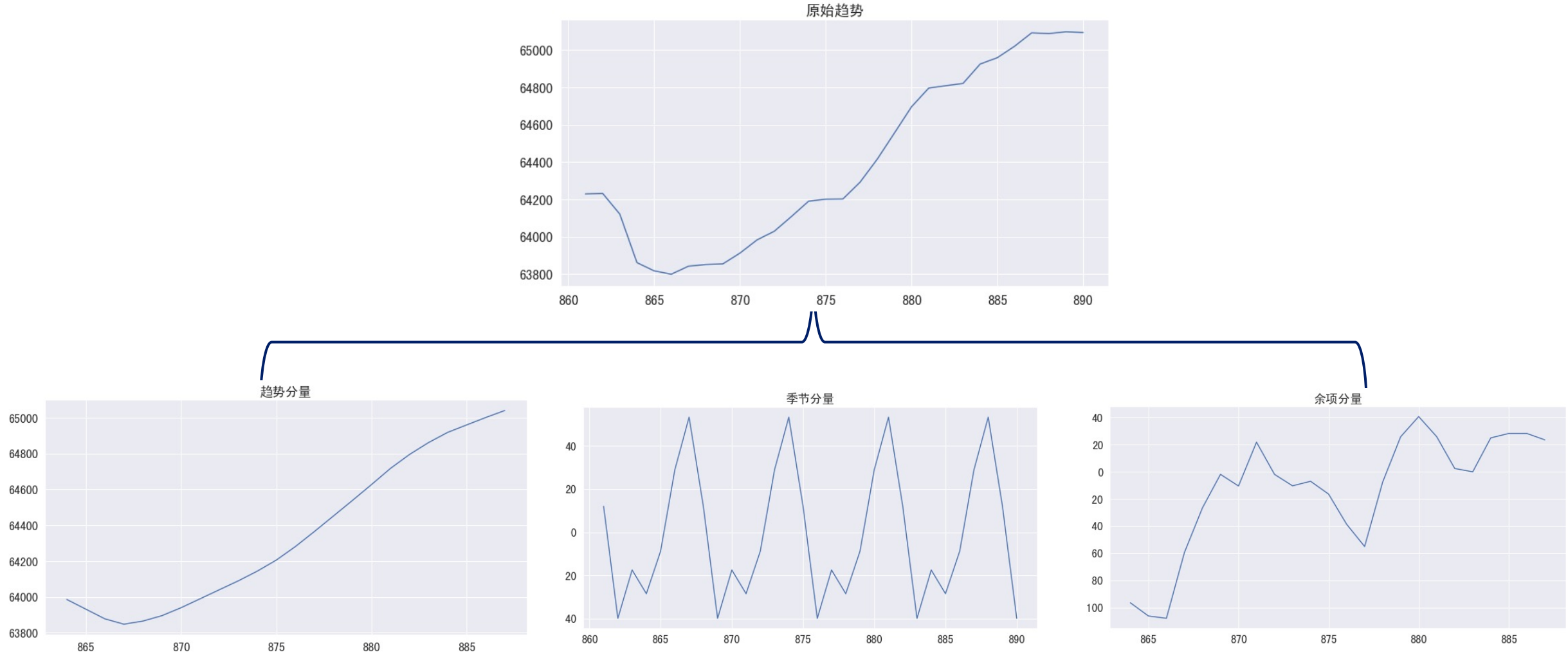

整体趋势图
count
60000
50000
40000
30000
2018-10 2019-01 2019-04 2019-07 2019-10 2020-01 2020-04 2020-07 2020-10 2021-01 2021-04 2021-07
ts


平滑后整体趋势图
count
65000
60000
55000
50000
45000
40000
35000
30000
25000
0
200
400
600
800


最近一周趋势图
count
65100
65050
65000
64950
64900
64850
2021-05-31 2021-06-01 2021-06-02 2021-06-03 2021-06-04 2021-06-05 2021-06-06 2021-06-07
ts


平滑后最近一周趋势图
count
64400
64350
64300
64250
64200
64150
882
884
886
888
890

解题：数据分解


原始趋势
65000
64800
64600
64400
64200
64000
63800
860
865
870
875
880
885
890
趋势分量
65000
64800
64600
64400
64200
64000
63800
865
870
875
880
885
季节分量
40
20
0
20
40
860
865
870
875
880
885
890
余项分量
40
20
0
20
40
60
80
100
865
870
875
880
885

解题演示

http://localhost:8888/notebooks/sharing.ipynb

总结讨论

- 用线性回归分析，对数据有什么要求？
- 数据不满足要求怎么办？
- 如何处理突变的数据？

案例二：人脸识别

How

人脸检测 → 人脸对齐 → 特征提取 → 特征比对

人脸检测

1

Resize image
生成图像金字塔

2

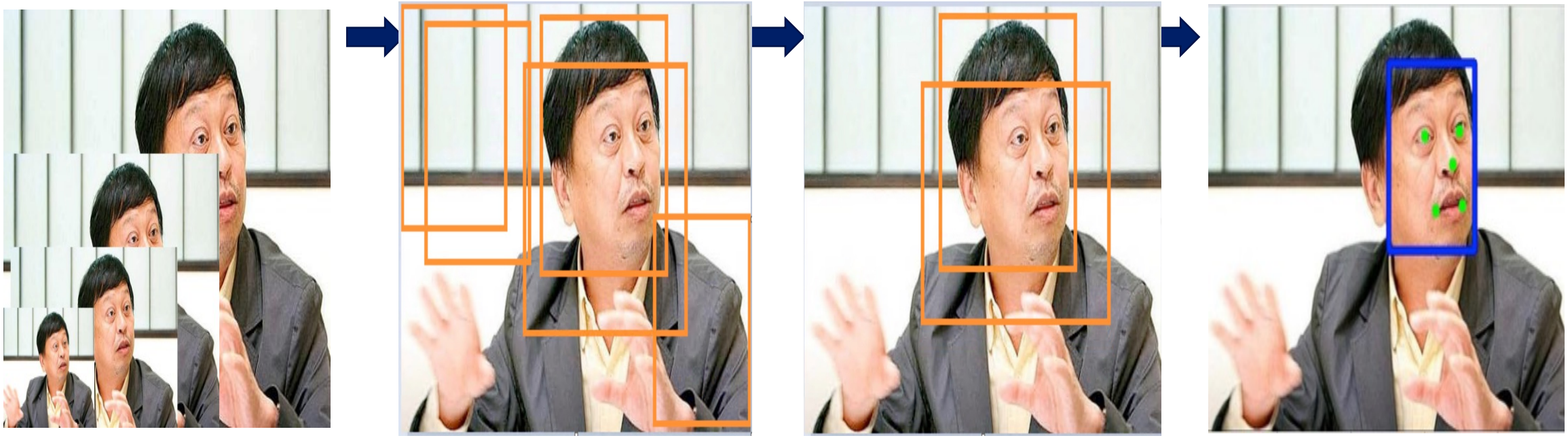
P-net
可能存在人脸区域

3

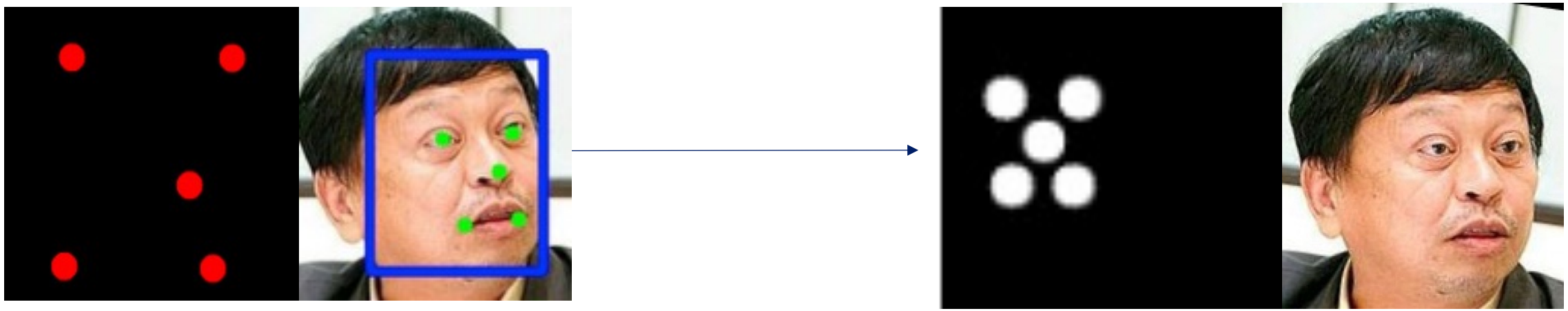
R-net
筛选人脸并修正位置

4

O-net
人脸位置和简单特征点



人脸对齐



1. 定位关键点（landmark 5）
2. 计算转换函数 (仿射矩阵)
3. 将原图map至目标图
4. 裁剪目标图中的人脸

特征提取


```
[0.04027741029858589, 0.08351167291402817,
0.005823252256959677, 0.0723235160112381,
0.028528105467557907, -0.002782160881906748,
-0.06524961441755295, 0.10399515926837921,
0.01219485979527235, 0.03158007934689522,
0.046927742660045624, -0.02802014909684658,
-0.03863518312573433, -0.0190310999751091,
0.005247218534350395, -0.03423447161912918,
0.06390134245157242, 0.043098170310258865,
-0.06691527366638184, 0.019953561946749687,
0.014163636602461338, 0.00026211352087557316,
-0.010168898850679398, -0.028404725715517998,
-0.04332667589187622, -0.01461505051702261,
0.06261993199586868, 0.0735521912574768,
0.030010586604475975, 0.061586856842041016,
-0.0013521158834919333, 0.02855655737221241,
0.020252032205462456, 0.0172031968832016,
0.004351011477410793, -0.08569888025522232,
-0.05994438752532005, -0.06681397557258606,
```

特征比对

```
[ 6.28630891e-02,  5.32379001e-02, -1.64854806e-02, -2.97333337e-02,
  1.53415222e-02,  7.81149277e-03, -4.99928966e-02,  2.11557243e-02,
 -3.02620642e-02, -1.29281655e-02,  1.52624073e-02,  4.54501994e-02,
  9.31495335e-03, -6.63329894e-03,  6.78491825e-03,  2.23199669e-02,
  4.74195331e-02,  6.79659769e-02, -2.03946736e-02,  2.52048057e-02,
  3.74105833e-02,  7.38691306e-03, -1.18066892e-02,  1.30082080e-02,
  2.29495578e-03, -2.15018168e-02,  4.13860902e-02, -1.24517158e-02,
 -1.86567474e-02,  6.72310665e-02,  1.10958636e-01, -4.03854176e-02,
  4.66009490e-02,  7.07942024e-02,  2.32276488e-02, -7.34092668e-02,
  6.29220903e-03, -5.19631915e-02,  3.17869112e-02,  2.12093536e-02,
 -1.84256416e-02, -8.80157799e-02,  1.68937305e-03,  2.51659099e-02,
 -7.35285506e-02,  1.42856846e-02, -5.51213548e-02,  5.96725801e-03,
 -6.49154047e-03,  3.56984772e-02, -4.21665125e-02, -2.19754670e-02,
 -1.01896562e-02, -4.22728211e-02,  4.17030193e-02, -4.52931896e-02,
  2.44072499e-03, -7.37402514e-02,  2.69813612e-02, -7.35680014e-03,
 -3.86550836e-02,  1.40417933e-01,  6.73008268e-04,  5.49310558e-02,
  2.46858057e-02, -7.52934366e-02, -2.27931142e-02, -4.06879149e-02,
  7.09813759e-02, -5.15609514e-04,  2.79082195e-03, -3.20651196e-03,
 -7.35983476e-02,  1.73214432e-02,  1.58355311e-02,  3.58786285e-02,
 -3.17432284e-02, -9.26326141e-02,  3.32418345e-02, -5.29297516e-02,
  1.55248661e-02, -6.22846372e-02,  4.85780044e-03, -9.41042788e-03,
```

```
[ 6.45104647e-02,  2.84561459e-02, -7.34514371e-02, -1.72763225e-02,
  1.13835242e-02, -1.63212884e-02, -5.34696281e-02,  5.32028750e-02,
 -1.44749098e-02,  3.59034464e-02,  1.85653958e-02,  5.90951927e-02,
  1.47780543e-02, -2.17742771e-02,  1.50234271e-02,  2.69742161e-02,
  9.79379192e-03,  6.51236475e-02, -4.73314198e-03,  1.31187811e-02,
  1.93645861e-02,  7.57417455e-02, -2.74137277e-02,  1.94943510e-02,
 -5.75501844e-03,  7.68118026e-03, -1.67309050e-03, -4.68759052e-02,
 -7.83467572e-03,  1.86435506e-02,  6.26649186e-02, -2.79785935e-02,
  6.60447478e-02,  7.25395456e-02,  3.40714306e-02, -3.05157658e-02,
  2.18674112e-02, -3.11621651e-02,  6.31265417e-02,  1.90785695e-02,
 -3.54125351e-02, -8.98810178e-02, -8.88275821e-03,  8.27952754e-03,
 -7.42505789e-02,  6.32991940e-02, -5.85555136e-02, -3.11240144e-02,
  7.45614385e-03,  3.36035006e-02, -3.36385928e-02, -3.62228416e-02,
 -2.25111637e-02, -3.21121365e-02,  1.06237046e-02, -3.13168541e-02,
  2.29744464e-02, -7.73122311e-02, -2.71368353e-03, -2.71095615e-02,
 -3.94065753e-02,  1.24143705e-01, -3.52797844e-02,  3.50417607e-02,
 -2.03845110e-02, -8.30745846e-02, -1.34285409e-02, -1.15193380e-02,
  8.32579955e-02,  6.08327519e-03,  1.97861549e-02, -4.40394022e-02,
 -4.70835753e-02,  3.52543071e-02,  3.41317244e-02, -1.77111034e-03,
```

$$Dist(a,b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots + (a_n - b_n)^2}$$

Demo与思考

http://localhost:8888/notebooks/face/demo.ipynb

- 隐私问题
- 能否借鉴到安全领域？

问题：哪个更难？

A：销售预测

B：人脸识别

C：目标追踪 http://localhost:8888/notebooks/trace.ipynb

D：智能音箱

当前AI智力水平如何？

翻译　Can bird fly？

Jenny: Do you love me？

Gump: Can bird fly？

感知
智能

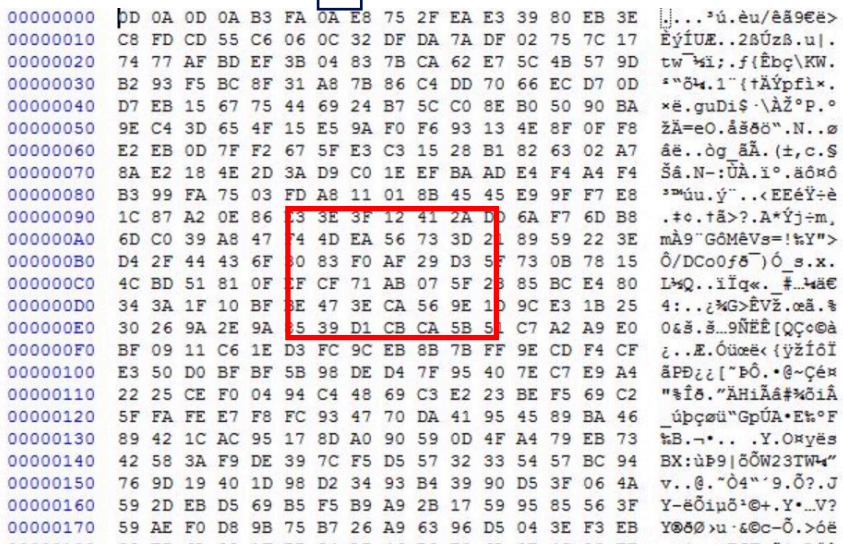
认知
智能

传统安全

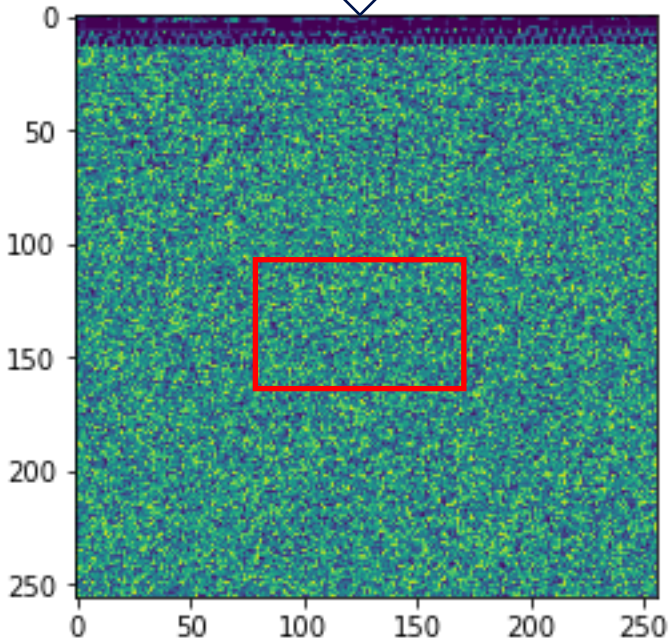
利用AI技术，改进安全检测方法

- File base detection
- Behavior analyse
- Obnormal detction
- Others

File base：B2M

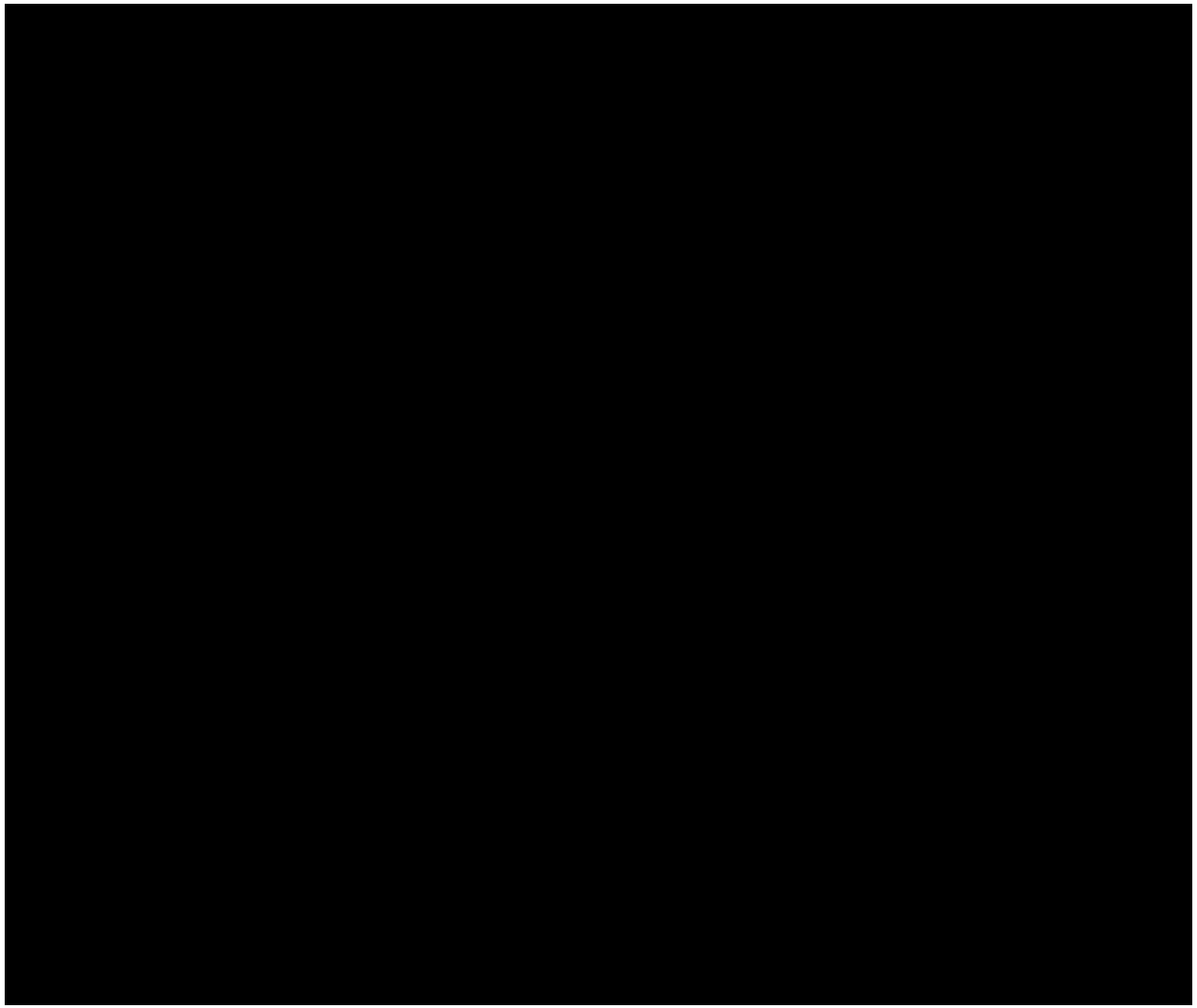


00000000	DD	0A	0D	0A	B3	FA	0A	E8	75	2F	EA	E3	39	80	EB	3E
00000010	C8	FD	CD	55	C6	06	0C	32	DF	DA	7A	DF	02	75	7C	17
00000020	74	77	AF	BD	EF	3B	04	83	7B	CA	62	E7	5C	4B	57	9D
00000030	B2	93	F5	BC	8F	31	A8	7B	86	C4	DD	70	66	EC	D7	0D
00000040	D7	EB	15	67	75	44	69	24	B7	5C	C0	8E	B0	50	90	BA
00000050	9E	C4	3D	65	4F	15	E5	9A	F0	F6	93	13	4E	8F	0F	F8
00000060	E2	EB	0D	7F	F2	67	5F	E3	C3	15	28	B1	82	63	02	A7
00000070	8A	E2	18	4E	2D	3A	D9	C0	1E	EF	BA	AD	E4	F4	A4	F4
00000080	B3	99	FA	75	03	FD	A8	11	01	8B	45	45	E9	9F	F7	E8
00000090	1C	87	A2	0E	86	13	3E	3F	12	41	2A	DD	6A	F7	6D	B8
000000A0	6D	C0	39	A8	47	14	4D	EA	56	73	3D	21	89	59	22	3E
000000B0	D4	2F	44	43	6F	00	83	F0	AF	29	D3	5F	73	0B	78	15
000000C0	4C	BD	51	81	0F	CF	CF	71	AB	07	5F	23	85	BC	E4	80
000000D0	34	3A	1F	10	BF	9E	47	3E	CA	56	9E	1D	9C	E3	1B	25
000000E0	30	26	9A	2E	9A	85	39	D1	CB	CA	5B	51	C7	A2	A9	E0
000000F0	BF	09	11	C6	1E	D3	FC	9C	EB	8B	7B	FF	9E	CD	F4	CF
00000100	E3	50	D0	BF	BF	5B	98	DE	D4	7F	95	40	7E	C7	E9	A4
00000110	22	25	CE	F0	04	94	C4	48	69	C3	E2	23	BE	F5	69	C2
00000120	5F	FA	FE	E7	F8	FC	93	47	70	DA	41	95	45	89	BA	46
00000130	89	42	1C	AC	95	17	8D	A0	90	59	0D	4F	A4	79	EB	73
00000140	42	58	3A	F9	DE	39	7C	F5	D5	57	32	33	54	57	BC	94
00000150	76	9D	19	40	1D	98	D2	34	93	B4	39	90	D5	3F	06	4A
00000160	59	2D	EB	D5	69	B5	F5	B9	A9	2B	17	59	95	85	56	3F
00000170	59	AE	F0	D8	9B	75	B7	26	A9	63	96	D5	04	3E	F3	EB



借鉴图像识别

内容分析



趨勢Projects

TW

CDC

PROD

https://safecircle.trendmicro.com/post/118320/share

新安全

AI技术带来了安全问题

- 隐私保护
- 模型训练
- 数据投毒

https://sandlab.cs.uchicago.edu/fawkes/#code

总结

1. Overview
2. Samples
3. AI and security

QQ

问题与讨论

Thanks

2021-7-20

Backlog

Backlog

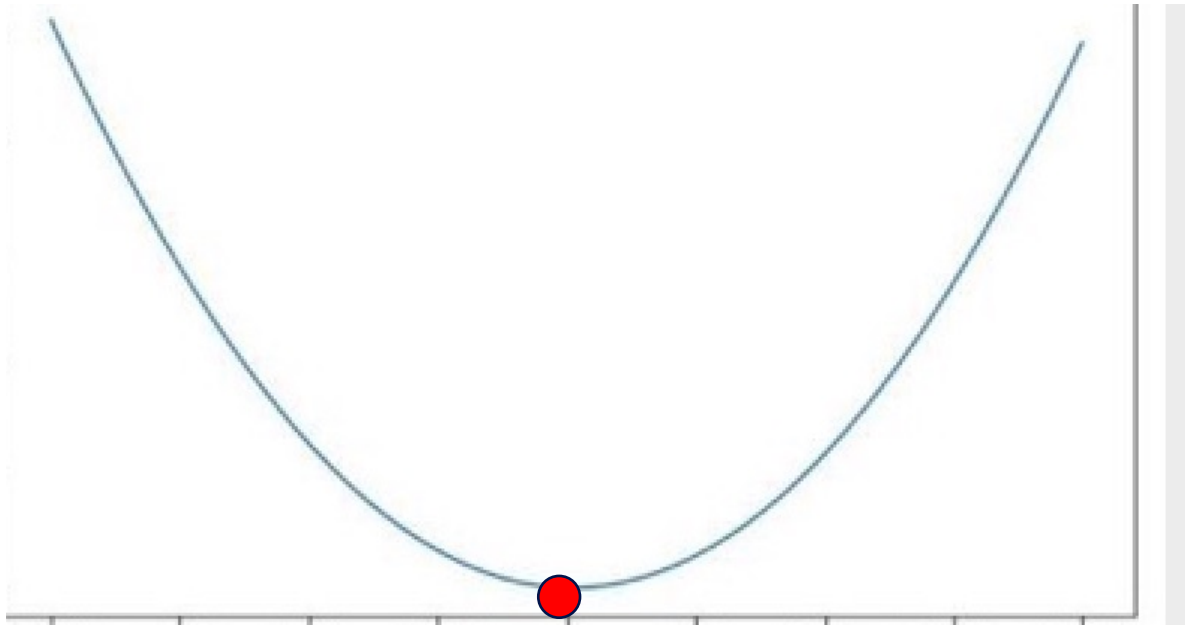
Preface

∑ Δ Ω ε

ω Ψ θ γ

Least square method

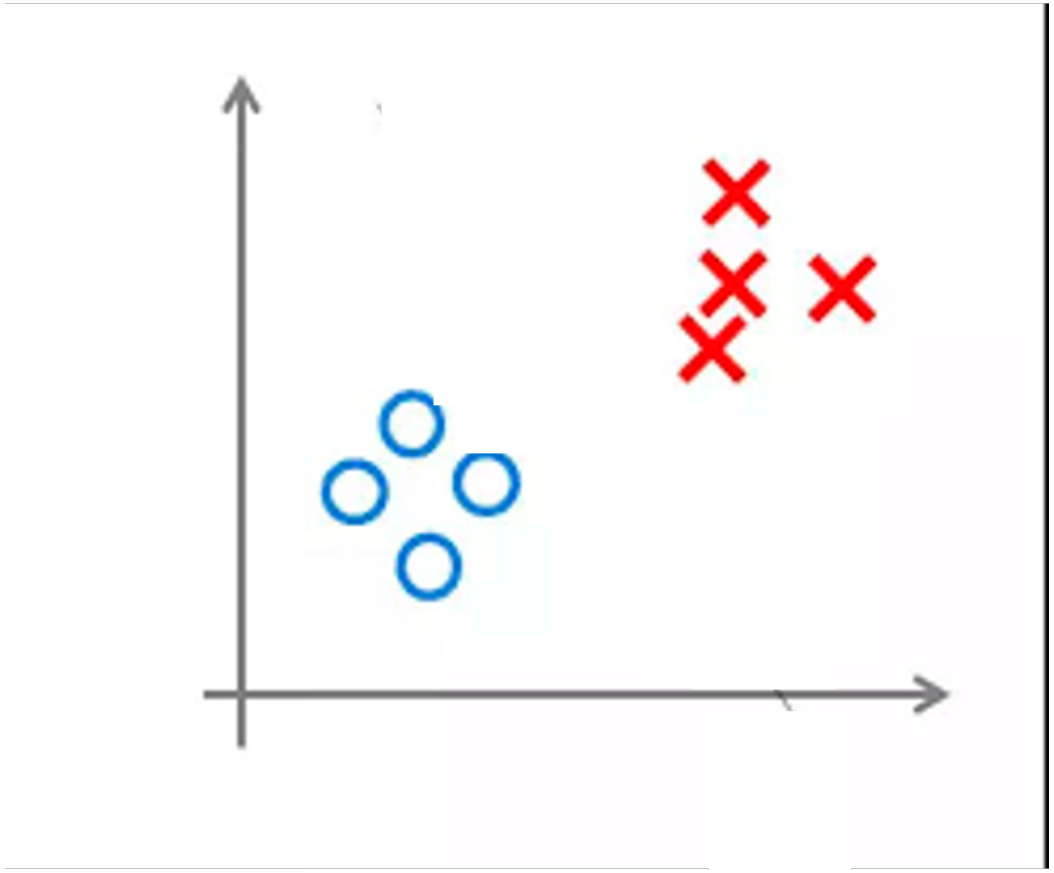
- F(x) = k* x + b
- Error = Real – Pred = Y- F(x)
- E(x) = Y- F(x) = Y - k * x + b
- J = $\sum E(x)^2$
- J(k , b) = $\frac{1}{2}\sum (Y - (k * x + b))^2$

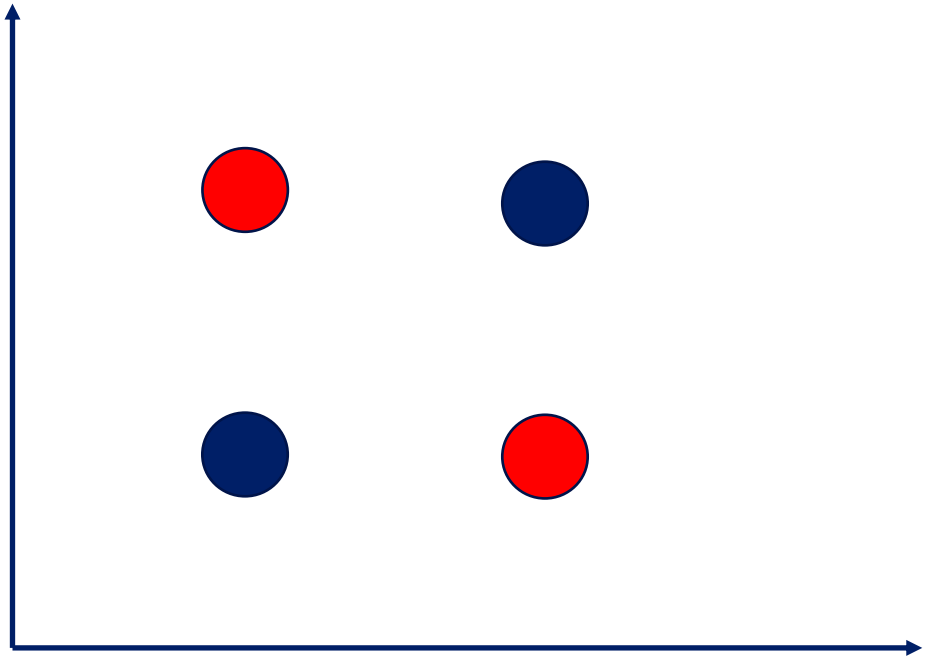


$\frac{\partial J}{\partial k} = 0, \frac{\partial J}{\partial b} = 0$

Find k,b value when error is minimum

异或问题





神经元