Inherent Tradeoffs in Learning Fair Representations

Han Zhao han.zhao@cs.cmu.edu Machine Learning Department, Carnegie Mellon University

COMPAS (Northpointe):

Recidivism risk assessment tool used in a county in Florida

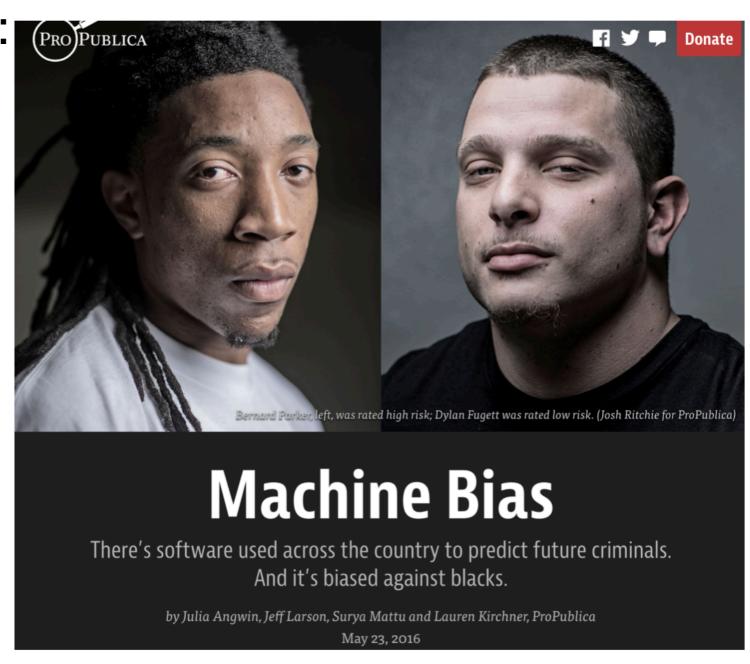
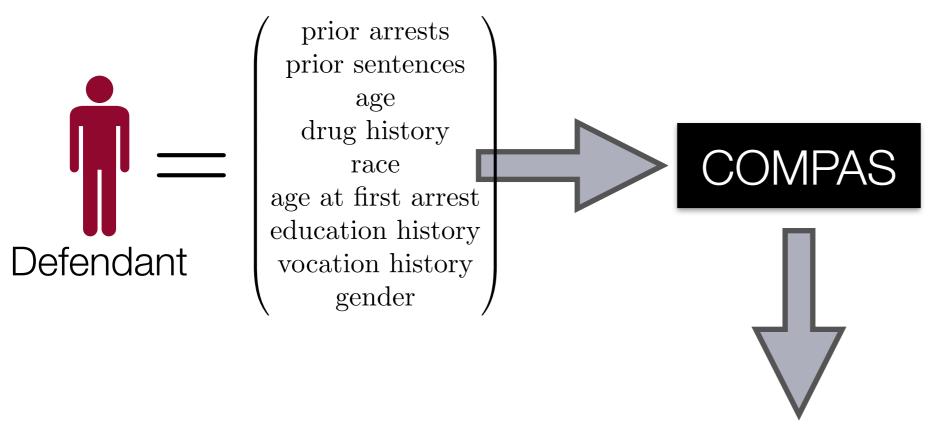


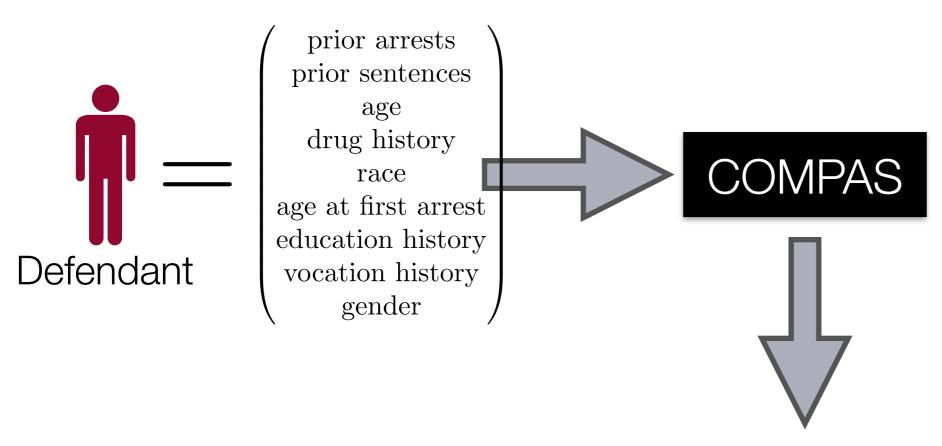
Figure credit: ProPublica, Larson et al., 2016

COMPAS (high level):



Risk score: $C(x) \in (0,1)$

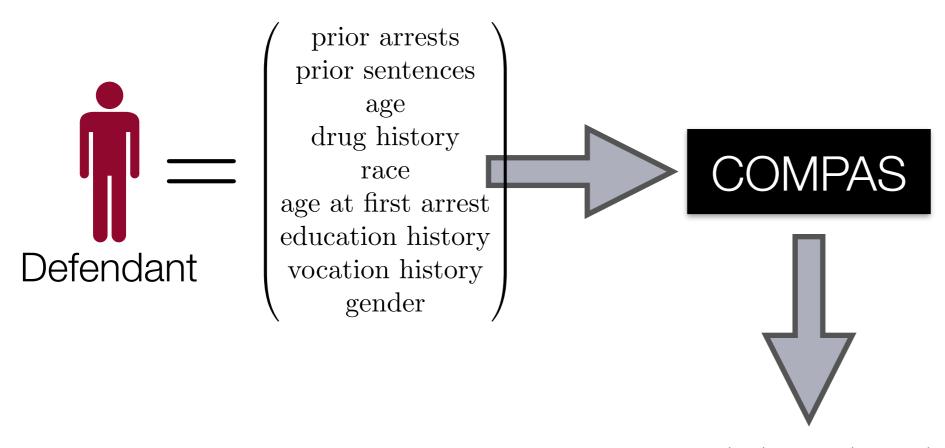
COMPAS (high level):



Risk score: $C(x) \in (0,1)$

- Risk score ~ likelihood of defendant to recidivate

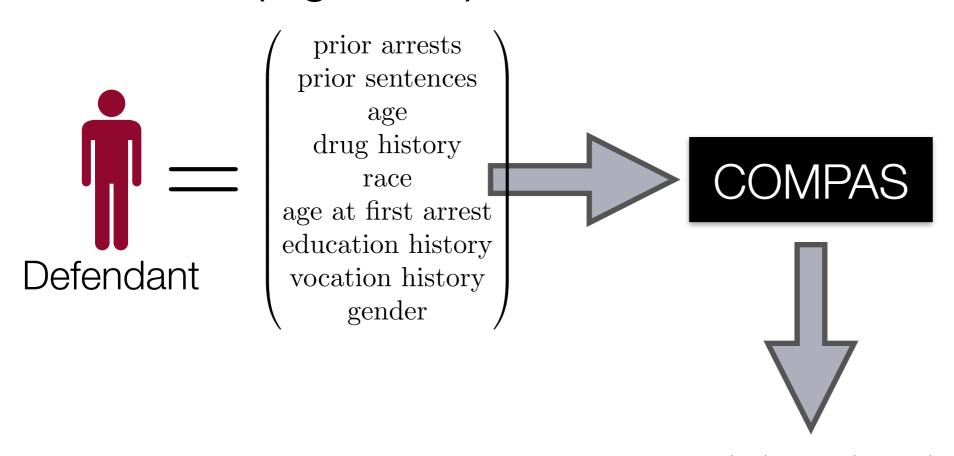
COMPAS (high level):



Risk score: $C(x) \in (0,1)$

- Risk score ~ likelihood of defendant to recidivate
- Inputs have (noisy) true label: 0 (not recidivate) / 1 (will recidivate)

COMPAS (high level):



Risk score: $C(x) \in (0,1)$

- Risk score ~ likelihood of defendant to recidivate
- Inputs have (noisy) true label: 0 (not recidivate) / 1 (will recidivate)
- The risk score + thresholding: 0 (low risk) / 1 (high risk)

ProPublica criticism:

	WHITE	AFRICAN AMERICAN
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

Overall, Northpointe's assessment tool correctly predicts recidivism 61 percent of the time. But blacks are almost twice as likely as whites to be labeled a higher risk but not actually re-offend. It makes the opposite mistake among whites: They are much more likely than blacks to be labeled lower risk but go on to commit other crimes. (Source: ProPublica analysis of data from Broward County, Fla.)

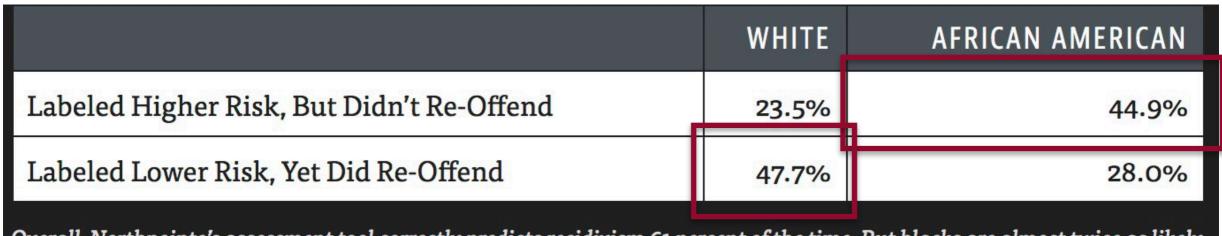
ProPublica criticism:

	WHITE	AFRICAN AMERICAN
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

Overall, Northpointe's assessment tool correctly predicts recidivism 61 percent of the time. But blacks are almost twice as likely as whites to be labeled a higher risk but not actually re-offend. It makes the opposite mistake among whites: They are much more likely than blacks to be labeled lower risk but go on to commit other crimes. (Source: ProPublica analysis of data from Broward County, Fla.)

Black defendants more likely than white to be incorrectly labeled "high risk"

ProPublica criticism:



Overall, Northpointe's assessment tool correctly predicts recidivism 61 percent of the time. But blacks are almost twice as likely as whites to be labeled a higher risk but not actually re-offend. It makes the opposite mistake among whites: They are much more likely than blacks to be labeled lower risk but go on to commit other crimes. (Source: ProPublica analysis of data from Broward County, Fla.)

- Black defendants more likely than white to be incorrectly labeled "high risk"
- White defendants more likely than black to be incorrectly labeled "low risk"

ProPublica criticism:



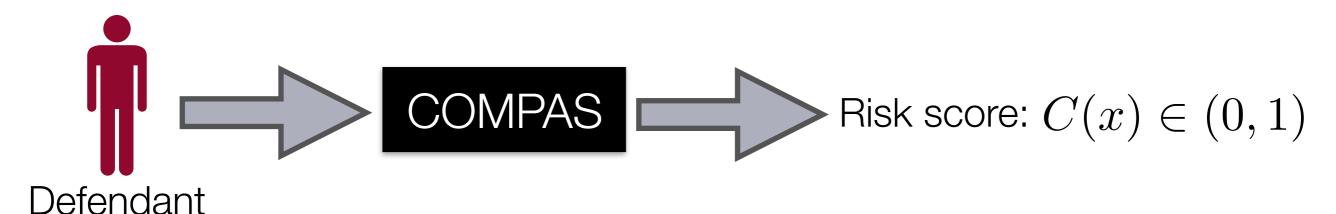
Overall, Northpointe's assessment tool correctly predicts recidivism 61 percent of the time. But blacks are almost twice as likely as whites to be labeled a higher risk but not actually re-offend. It makes the opposite mistake among whites: They are much more likely than blacks to be labeled lower risk but go on to commit other crimes. (Source: ProPublica analysis of data from Broward County, Fla.)

- Black defendants more likely than white to be incorrectly labeled "high risk"
- White defendants more likely than black to be incorrectly labeled "low risk"

Bias: Disparate FPR/FNR across groups!

Northpointes' defense:

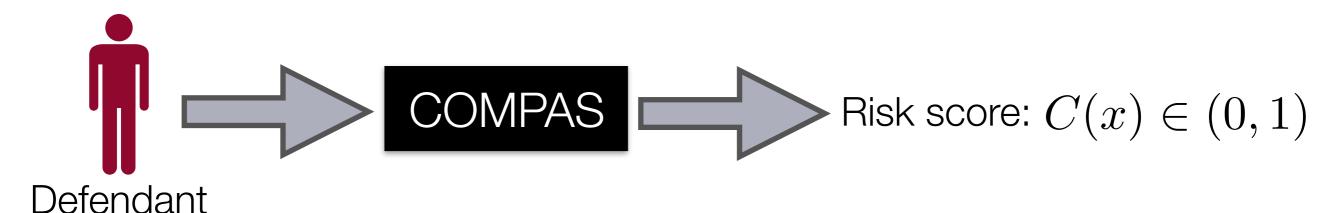
Defendants labeled as "high risk" **equally likely** to recidivate, regardless of race



- The COMPAS tool C(x) is statistically calibrated by group

Northpointes' defense:

Defendants labeled as "high risk" **equally likely** to recidivate, regardless of race

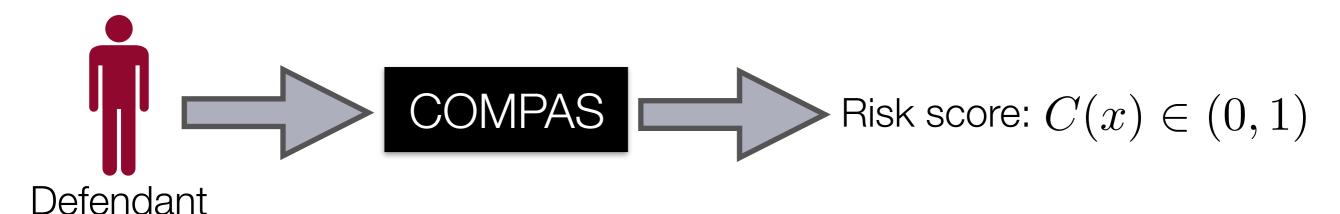


- The COMPAS tool C(x) is statistically calibrated by group
- Let $A \in \{0,1\}$ be the group membership (race), $Y \in \{0,1\}$ be the true label (recidivism), then

$$\forall a \in \{0, 1\}, \forall c \in (0, 1), \quad \Pr(Y = 1 \mid C(x) = c, A = a) = c$$

Northpointes' defense:

Defendants labeled as "high risk" **equally likely** to recidivate, regardless of race



- The COMPAS tool C(x) is statistically calibrated by group
- Let $A \in \{0,1\}$ be the group membership (race), $Y \in \{0,1\}$ be the true label (recidivism), then

$$\forall a \in \{0, 1\}, \forall c \in (0, 1), \quad \Pr(Y = 1 \mid C(x) = c, A = a) = c$$

No Bias: Equal treatment!

Fundamental incompatibility between different notions of fairness:

- True label: $Y \in \{0, 1\}$
- Group membership: $A \in \{0, 1\}$
- Probabilistic classifier: $\widehat{Y} \in (0,1)$ or binary classifier: $\widehat{Y} \in \{0,1\}$
- Base rate: $Pr(Y = 1 \mid A = a), \ a \in \{0, 1\}$
- Difference of base rates:

$$\Delta_{\rm BR} = |\Pr(Y = 1 \mid A = 0) - \Pr(Y = 1 \mid A = 1)|$$

Fundamental incompatibility between different notions of fairness:

- True label: $Y \in \{0, 1\}$
- Group membership: $A \in \{0, 1\}$
- Probabilistic classifier: $\widehat{Y} \in (0,1)$ or binary classifier: $\widehat{Y} \in \{0,1\}$
- Base rate: $Pr(Y = 1 \mid A = a), \ a \in \{0, 1\}$
- Difference of base rates:

$$\Delta_{\rm BR} = |\Pr(Y = 1 \mid A = 0) - \Pr(Y = 1 \mid A = 1)|$$

Theorem (Chouldechova'17, Kleinberg, Mullainathan, Raghavan'16): Statistical calibration and Equalized FPR/FNR cannot hold simultaneously unless $\Delta_{\rm BR}=0$ ($A\perp Y$) or $\widehat{Y}=Y$ (perfect prediction).

Lesson learned:

Depending on the problem, choose the appropriate criterion

Lesson learned:

Depending on the problem, choose the appropriate criterion

But, there are just too many definitions...

Lesson learned:

Depending on the problem, choose the appropriate criterion

But, there are just too many definitions...





I wrote up a 2-pager titled "21 fairness definitions and their politics" based on the tweetstorm below and it was accepted at a tutorial for the Conference on Fairness, Accountability, and Transparency!

Here it is (with minor edits):

docs.google.com/document/d/1bn ...

See you on Feb 23/24.

Arvind Narayanan ② @random_walker
When I tell my computer science colleagues that there are so many fairness definitions, they are often surprised and/or confused. [Thread] twitter.com/random_walker/...
显示这个主题帖

Lesson learned:

Depending on the problem, choose the appropriate criterion

But, there are just too many definitions...





I wrote up a 2-pager titled "21 fairness definitions and their politics" based on the tweetstorm below and it was accepted at a tutorial for the Conference on Fairness, Accountability, and Transparency!

Here it is (with minor edits):

docs.google.com/document/d/1bn ... See you on Feb 23/24.

Arvind Narayanan Ograndom_walker

When I tell my computer science colleagues that there are so many fairness definitions, they are often surprised and/or confused. [Thread] twitter.com/random_walker/...

Paper	Citation #
[12]	208
[11]	29
[10]	57
[10]	57
[10]	57
[14]	106
[8]	18
[8]	18
[8]	18
[10]	57
[16]	81
[16]	81
[16]	81
	[12] [11] [10] [10] [10] [14] [8] [8] [8] [10] [16] [16]

Lesson learned:

Depending on the problem, choose the appropriate criterion

But, there are just too many definitions...



正在关注

I wrote up a 2-pager titled "21 fairness definitions and their politics" based on the tweetstorm below and it was accepted at a tutorial for the Conference on Fairness, Accountability, and Transparency!

Here it is (with minor edits):

docs.google.com/document/d/1bn ... See you on Feb 23/24.

Arvind Narayanan 🔮 @random_walker

When I tell my computer science colleagues that there are so many fairness definitions, they are often surprised and/or confused. [Thread] twitter.com/random_walker/...

Paper	Citation #
[12]	208
[11]	29
[10]	57
[10]	57
[10]	57
[14]	106
[8]	18
[8]	18
[8]	18
[10]	57
[16]	81
[16]	81
[16]	81
	[12] [11] [10] [10] [10] [14] [8] [8] [8] [10] [16] [16]

Lesson learned:

Depending on the problem, choose the appropriate criterion

But, there are just too many definitions...



正在关注

I wrote up a 2-pager titled "21 fairness definitions and their politics" based on the tweetstorm below and it was accepted at a tutorial for the Conference on Fairness, Accountability, and Transparency!

Here it is (with minor edits):

docs.google.com/document/d/1bn ... See you on Feb 23/24.

Arvind Narayanan @random_walker

When I tell my computer science colleagues that there are so many fairness definitions, they are often surprised and/or confused. [Thread] twitter.com/random_walker/...

Paper	Citation #
[12]	208
[11]	29
[10]	57
[10]	57
[10]	57
[14]	106
[8]	18
[8]	18
[8]	18
[10]	57
[16]	81
[16]	81
[16]	81
	[12] [11] [10] [10] [10] [14] [8] [8] [8] [10] [16] [16]

Lesson learned:

Depending on the problem, choose the appropriate criterion

But, there are just too many definitions...



正在关注

I wrote up a 2-pager titled "21 fairness definitions and their politics" based on the tweetstorm below and it was accepted at a tutorial for the Conference on Fairness, Accountability, and Transparency!

Here it is (with minor edits):

docs.google.com/document/d/1bn ... See you on Feb 23/24.

Arvind Narayanan 🔮 @random_walker

When I tell my computer science colleagues that there are so many fairness definitions, they are often surprised and/or confused. [Thread] twitter.com/random_walker/...

Definition	Paper	Citation #
Group fairness or statistical parity	[12]	208
Conditional statistical parity	[11]	29
Predictive parity	[10]	57
False positive error rate balance	[10]	57
False negative error rate balance	[10]	57
Equalised odds	[14]	106
Conditional use accuracy equality	[8]	18
Overall accuracy equality	[8]	18
Treatment equality	[8]	18
Test-fairness or calibration	[10]	57
Well calibration	[16]	81
Balance for positive class	[16]	81
Balance for negative class	[16]	81

Statistical parity (demographic parity):

$$\widehat{Y} \perp A$$

The prediction given by an algorithm shouldn't take the sensitive attribute A into account

- College admission: affirmative action
- Movie recommendation

- ...

Statistical parity (demographic parity):

$$\widehat{Y} \perp A$$

The prediction given by an algorithm shouldn't take the sensitive attribute A into account

- College admission: affirmative action
- Movie recommendation
- ...

How to achieve statistical parity while preserving utility?

Statistical parity (demographic parity): $\widehat{Y} \perp A$

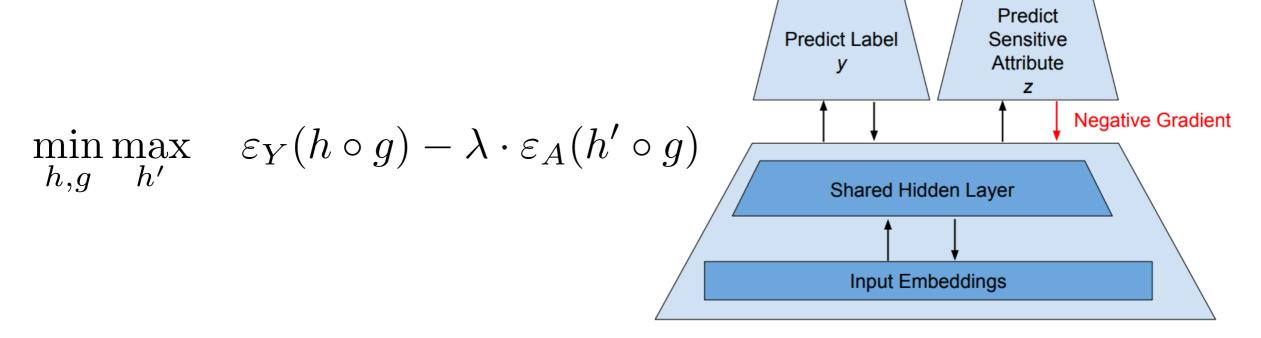
$$\widehat{Y} \perp A \Leftrightarrow I(\widehat{Y}; A) = 0 \Leftrightarrow \Pr(\widehat{Y} \mid A = 0) = \Pr(\widehat{Y} \mid A = 1)$$

So it suffices if we could learn invariant representations Z that is independent of A, then any predictor \widehat{Y} upon Z should be independent of A as well

Statistical parity (demographic parity): $\widehat{Y} \perp A$

$$\widehat{Y} \perp A \Leftrightarrow I(\widehat{Y}; A) = 0 \Leftrightarrow \Pr(\widehat{Y} \mid A = 0) = \Pr(\widehat{Y} \mid A = 1)$$

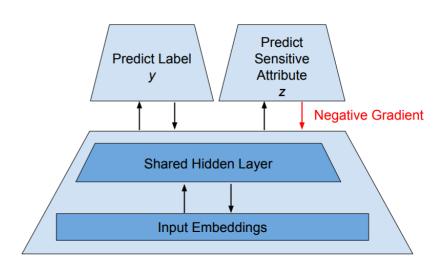
So it suffices if we could learn invariant representations Z that is independent of A, then any predictor \widehat{Y} upon Z should be independent of A as well



Minimax optimization formulation:

$$\min_{h,g} \max_{h'} \quad \varepsilon_Y(h \circ g) - \lambda \cdot \varepsilon_A(h' \circ g)$$

In practice, the loss function $\varepsilon(\cdot)$ is often chosen as the crossentropy loss

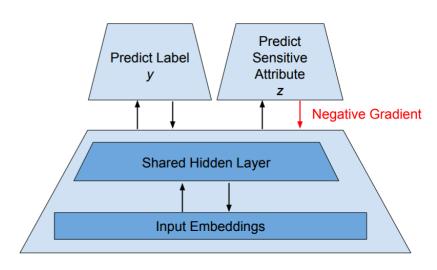


Minimax optimization formulation:

$$\min_{h,g} \max_{h'} \quad \varepsilon_Y(h \circ g) - \lambda \cdot \varepsilon_A(h' \circ g)$$

In practice, the loss function $\varepsilon(\cdot)$ is often chosen as the crossentropy loss

- Shared representations Z = g(X)

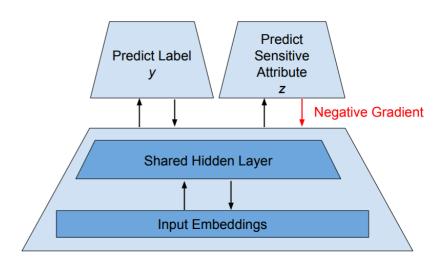


Minimax optimization formulation:

$$\min_{h,g} \max_{h'} \quad \varepsilon_Y(h \circ g) - \lambda \cdot \varepsilon_A(h' \circ g)$$

In practice, the loss function $\varepsilon(\cdot)$ is often chosen as the crossentropy loss

- Shared representations Z = g(X)
- For any fixed Z=g(X), the optimal h,h^\prime is given by the corresponding conditional distribution



Minimax optimization formulation:

$$\min_{h,g} \max_{h'} \quad \varepsilon_Y(h \circ g) - \lambda \cdot \varepsilon_A(h' \circ g)$$

In practice, the loss function $\varepsilon(\cdot)$ is often chosen as the crossentropy loss

- Shared representations Z = g(X)
- For any fixed Z=g(X), the optimal h,h^\prime is given by the corresponding conditional distribution

$$h(Z) = \Pr(Y = 1 \mid Z); \quad h'(Z) = \Pr(A = 1 \mid Z) \text{Predict Label Predict Label Negative Gradient}$$
 Negative Gradient Input Embeddings

Simplified optimization:

$$\min_{Z=g(X)} \quad H(Y\mid Z) - \lambda \cdot H(A\mid Z)$$

Clearly, the optimal solution depends on the "coupling" between A,Y:

Simplified optimization:

$$\min_{Z=g(X)} \quad H(Y\mid Z) - \lambda \cdot H(A\mid Z)$$

Clearly, the optimal solution depends on the "coupling" between A, Y:

- If $A=Y,\ a.s.$, then we cannot hope to find a good tradeoff

Simplified optimization:

$$\min_{Z=g(X)} \quad H(Y\mid Z) - \lambda \cdot H(A\mid Z)$$

Clearly, the optimal solution depends on the "coupling" between A, Y:

- If A = Y, a.s., then we cannot hope to find a good tradeoff
- If $A \perp Y$, then we can preserve information about Y while filtering out information related to A

Simplified optimization:

$$\min_{Z=g(X)} \quad H(Y\mid Z) - \lambda \cdot H(A\mid Z)$$

Clearly, the optimal solution depends on the "coupling" between A, Y:

- If A = Y, a.s., then we cannot hope to find a good tradeoff
- If $A \perp Y$, then we can preserve information about Y while filtering out information related to A

In general, tradeoff exists between fairness and utility

Theorem: If $\widehat{Y} = (h \circ g)(X)$ satisfies statistical parity, then $\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \geq \Delta_{\operatorname{BR}}$

Theorem: If $\widehat{Y} = (h \circ g)(X)$ satisfies statistical parity, then

$$\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \ge \Delta_{\operatorname{BR}}$$

- $\operatorname{Err}_a(h \circ g)$ is the true binary classification error conditioned on group A = a

$$\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \ge \Delta_{\operatorname{BR}}$$

- $\operatorname{Err}_a(h \circ g)$ is the true binary classification error conditioned on group A = a
- Recall $\Delta_{\rm BR}=|\Pr(Y=1\mid A=0)-\Pr(Y=1\mid A=1)|$ measures the difference of the base rates

$$\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \ge \Delta_{\operatorname{BR}}$$

- $\operatorname{Err}_a(h \circ g)$ is the true binary classification error conditioned on group A = a
- Recall $\Delta_{\rm BR}=|\Pr(Y=1\mid A=0)-\Pr(Y=1\mid A=1)|$ measures the difference of the base rates
- Interpretation: cannot simultaneously minimize errors on both groups, has to sacrifice accuracy on one of the (minority) group if we enforce statistical parity

$$\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \ge \Delta_{\operatorname{BR}}$$

- $\operatorname{Err}_a(h \circ g)$ is the true binary classification error conditioned on group A = a
- Recall $\Delta_{\rm BR}=|\Pr(Y=1\mid A=0)-\Pr(Y=1\mid A=1)|$ measures the difference of the base rates
- Interpretation: cannot simultaneously minimize errors on both groups, has to sacrifice accuracy on one of the (minority) group if we enforce statistical parity
- If A=Y, then $\Delta_{\mathrm{BR}}=1$, meaning $\max\{\mathrm{Err}_0(h\circ g),\mathrm{Err}_1(h\circ g)\}\geq 0.5$

$$\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \ge \Delta_{\operatorname{BR}}$$

- $\operatorname{Err}_a(h \circ g)$ is the true binary classification error conditioned on group A = a
- Recall $\Delta_{\rm BR}=|\Pr(Y=1\mid A=0)-\Pr(Y=1\mid A=1)|$ measures the difference of the base rates
- Interpretation: cannot simultaneously minimize errors on both groups, has to sacrifice accuracy on one of the (minority) group if we enforce statistical parity
- If A=Y, then $\Delta_{\mathrm{BR}}=1$, meaning $\max\{\mathrm{Err}_0(h\circ g),\mathrm{Err}_1(h\circ g)\}\geq 0.5$
- If $A \perp Y$, then $\Delta_{\rm BR} = 0$, lower bound gracefully degrades to 0, i.e., no constraint on utility

Approximate version exists as well, consider:

$$X \xrightarrow{g} Z \xrightarrow{h} \hat{Y}$$

Then the following lower bounds hold:

$$\operatorname{Err}_0(h \circ g) + \operatorname{Err}_1(h \circ g) \ge \Delta_{\operatorname{BR}} - \Delta_{\operatorname{DP}}(\widehat{Y})$$

where

$$\Delta_{\mathrm{DP}}(\widehat{Y}) = \left| \Pr(\widehat{Y} = 1 \mid A = 0) - \Pr(\widehat{Y} = 1 \mid A = 1) \right|$$

is an approximate version of statistical parity (demographic parity)

Approximate version exists as well, consider:

$$X \xrightarrow{g} Z \xrightarrow{h} \hat{Y}$$

Define f-divergence between distribution \mathcal{P} and \mathcal{Q} :

$$D_f(\mathcal{P} \parallel \mathcal{Q}) = \mathbb{E}_{\mathcal{Q}} \left[f\left(\frac{d\mathcal{P}}{d\mathcal{Q}}\right) \right]$$

where f(1) = 0 and is convex

Approximate version exists as well, consider:

$$X \xrightarrow{g} Z \xrightarrow{h} \hat{Y}$$

Define f-divergence between distribution \mathcal{P} and \mathcal{Q} :

$$D_f(\mathcal{P} \parallel \mathcal{Q}) = \mathbb{E}_{\mathcal{Q}} \left[f \left(\frac{d\mathcal{P}}{d\mathcal{Q}} \right) \right]$$

where f(1) = 0 and is convex

Name	$D_f(\mathcal{P} \parallel \mathcal{Q})$	Generator $f(t)$	Symm.	Tri.
Kullback-Leibler	$D_{\mathrm{KL}}(\mathcal{P} \mid\mid \mathcal{Q})$	$t \log t$	X	X
Reverse-KL	$D_{\mathrm{KL}}(\mathcal{Q} \mathcal{P})$	$-\log t$	X	X
Jensen-Shannon	$D_{\text{JS}}(\mathcal{P},\mathcal{Q}) := \frac{1}{2}(D_{\text{KL}}(\mathcal{P} \mathcal{M}) + D_{\text{KL}}(\mathcal{Q} \mathcal{M}))$	$t\log t - (t+1)\log(\tfrac{t+1}{2})$	✓	X
Squared Hellinger	$H^2(\mathcal{P},\mathcal{Q}) := rac{1}{2} \int (\sqrt{d\mathcal{P}} - \sqrt{d\mathcal{Q}})^2$	$(1-\sqrt{t})^2/2$	✓	X
Total Variation	$d_{\mathrm{TV}}(\mathcal{P},\mathcal{Q}) \coloneqq \sup_{E} \mathcal{P}(E) - \mathcal{Q}(E) $	t-1 /2	✓	✓

Approximate version exists as well, consider:

$$X \xrightarrow{g} Z \xrightarrow{h} \hat{Y}$$

We can also measure the tradeoff in terms of invariant representations: (Informal) If $g_{\sharp}\mathcal{D}_{0}$ and $g_{\sharp}\mathcal{D}_{1}$ are sufficient close to each other, then:

Total variation lower bound:

$$\operatorname{Err}_{0}(h \circ g) + \operatorname{Err}_{1}(h \circ g) \geq d_{\operatorname{TV}}(\mathcal{D}_{0}(Y), \mathcal{D}_{1}(Y)) - d_{\operatorname{TV}}(g_{\#}\mathcal{D}_{0}, g_{\#}\mathcal{D}_{1})$$

Jensen-Shannon lower bound:

$$\operatorname{Err}_{0}(h \circ g) + \operatorname{Err}_{1}(h \circ g) \geq (d_{\operatorname{JS}}(\mathcal{D}_{0}(Y), \mathcal{D}_{1}(Y)) - d_{\operatorname{JS}}(g_{\#}\mathcal{D}_{0}, g_{\#}\mathcal{D}_{1}))^{2}/2$$

Hellinger lower bound:

$$\operatorname{Err}_{0}(h \circ g) + \operatorname{Err}_{1}(h \circ g) \geq (H(\mathcal{D}_{0}(Y), \mathcal{D}_{1}(Y)) - H(g_{\sharp}\mathcal{D}_{0}, g_{\sharp}\mathcal{D}_{1}))^{2}/2$$

Approximate version exists as well, consider:

$$X \xrightarrow{g} Z \xrightarrow{h} \hat{Y}$$

We can also measure the tradeoff in terms of invariant representations: (Informal) If $g_{\sharp}\mathcal{D}_{0}$ and $g_{\sharp}\mathcal{D}_{1}$ are sufficient close to each other, then:

Total variation lower bound:

$$\operatorname{Err}_{0}(h \circ g) + \operatorname{Err}_{1}(h \circ g) \geq d_{\operatorname{TV}}(\mathcal{D}_{0}(Y), \mathcal{D}_{1}(Y)) - d_{\operatorname{TV}}(g_{\#}\mathcal{D}_{0}, g_{\#}\mathcal{D}_{1})$$

Jensen-Shannon lower bound:

$$\operatorname{Err}_{0}(h \circ g) + \operatorname{Err}_{1}(h \circ g) \geq (d_{\operatorname{JS}}(\mathcal{D}_{0}(Y), \mathcal{D}_{1}(Y)) - d_{\operatorname{JS}}(g_{\#}\mathcal{D}_{0}, g_{\#}\mathcal{D}_{1}))^{2}/2$$

Hellinger lower bound:

$$\operatorname{Err}_{0}(h \circ g) + \operatorname{Err}_{1}(h \circ g) \geq \left(H\left(\mathcal{D}_{0}(Y), \mathcal{D}_{1}(Y)\right) - H\left(g_{\sharp}\mathcal{D}_{0}, g_{\sharp}\mathcal{D}_{1}\right)\right)^{2}/2$$

The more invariant the representations, the worse the joint error

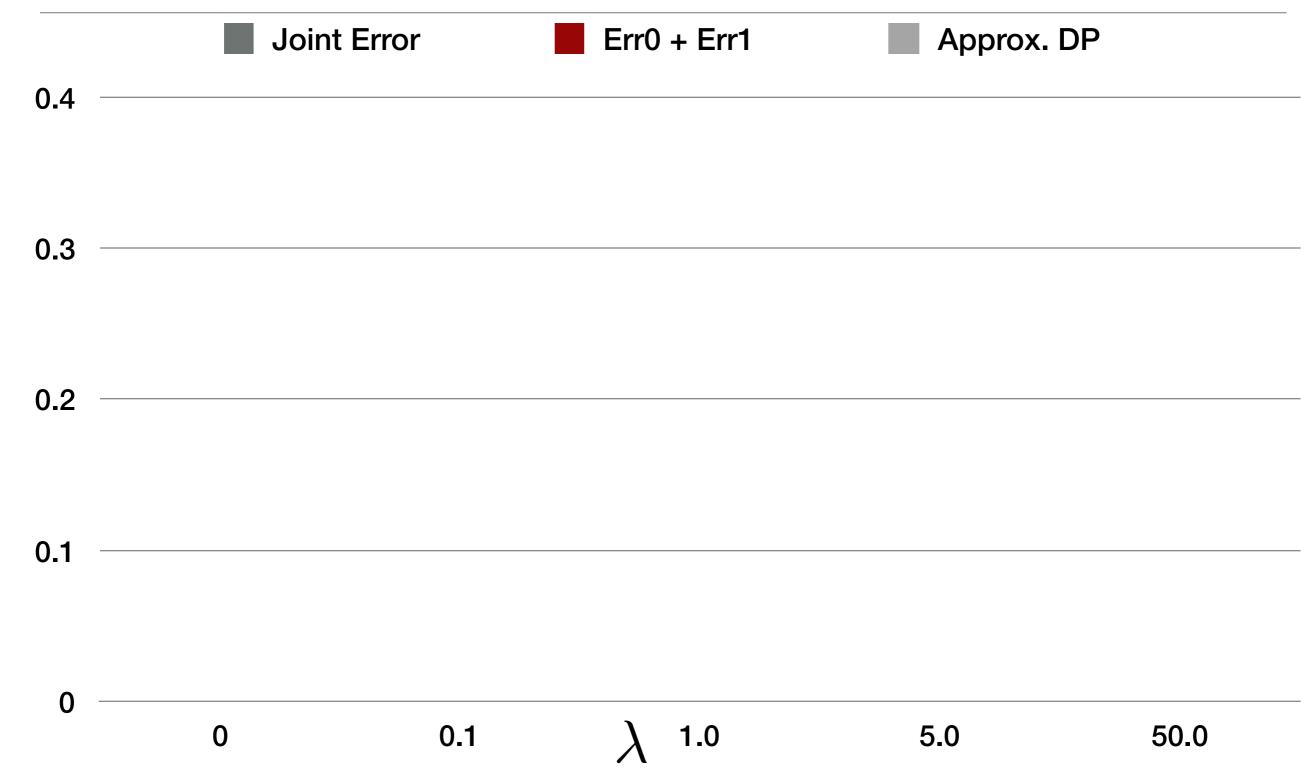
Income Prediction: Adult dataset

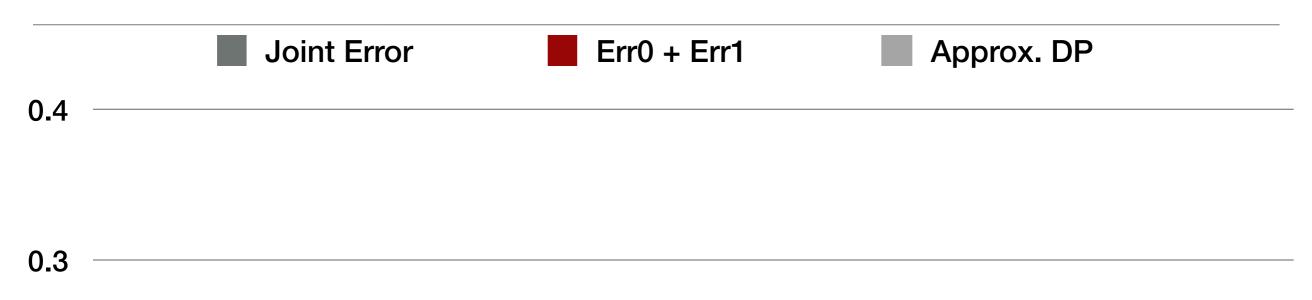
- Train/Test: 30,162/15,060 adults information collected in a 1994 census
- Target variable: Y=1 iff annual income > 50K
- Sensitive variable: A = 0/1 = Male/Female
- Other attributes: age, education, etc.
- Base rates are different across groups:

$$Pr(Y = 1 \mid A = 0) = 0.310$$
 $Pr(Y = 1 \mid A = 1) = 0.113$

- Imbalanced marginal distribution:

$$\Pr(A=0) = 0.673$$

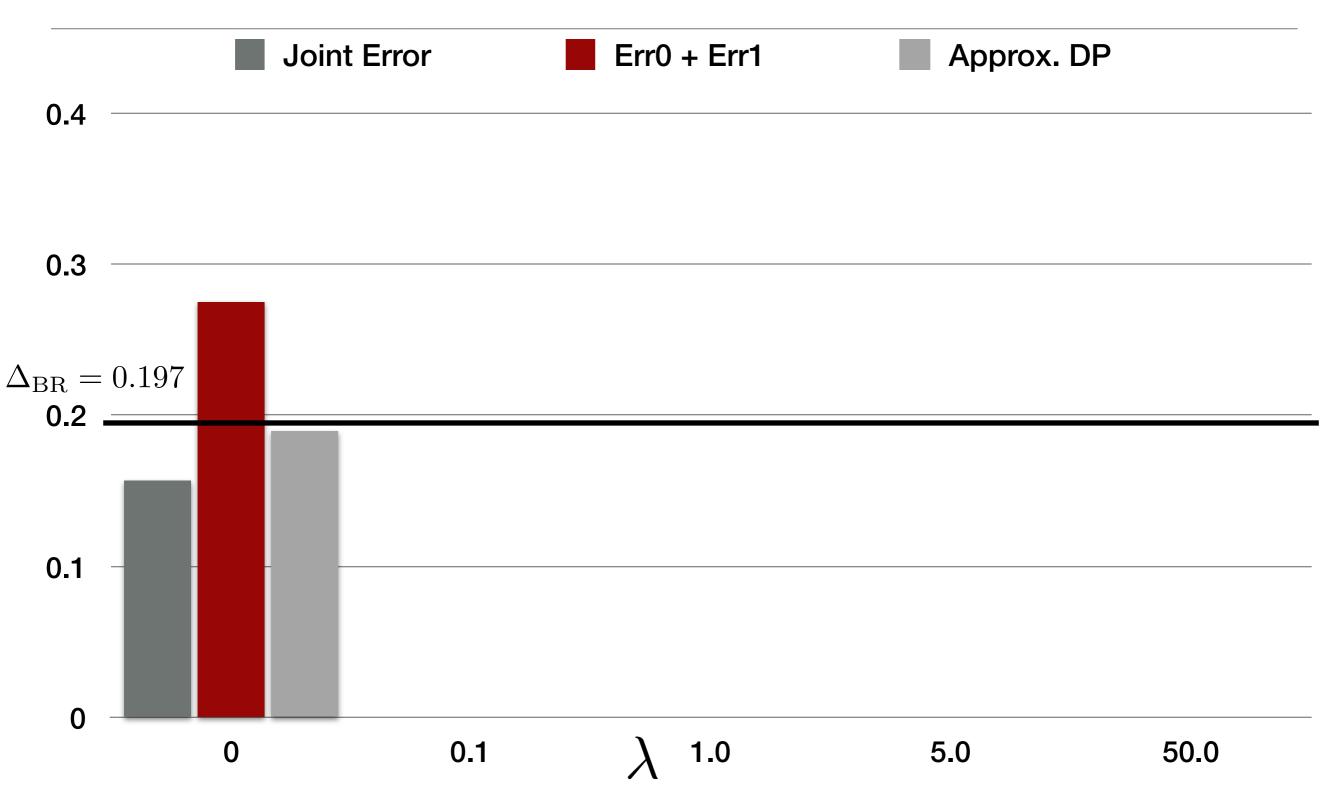


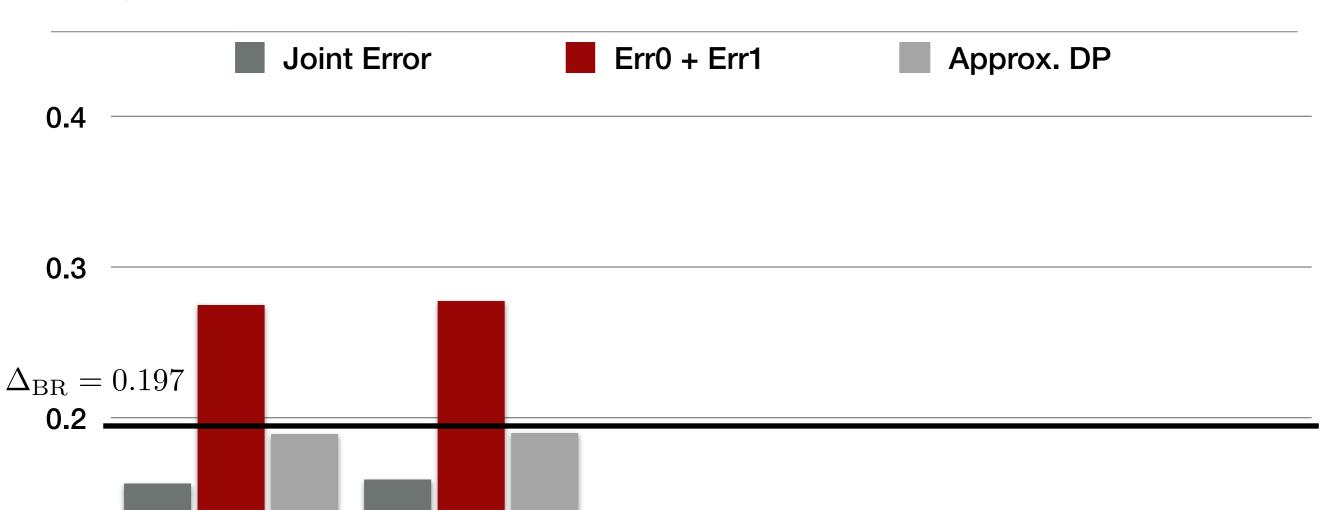


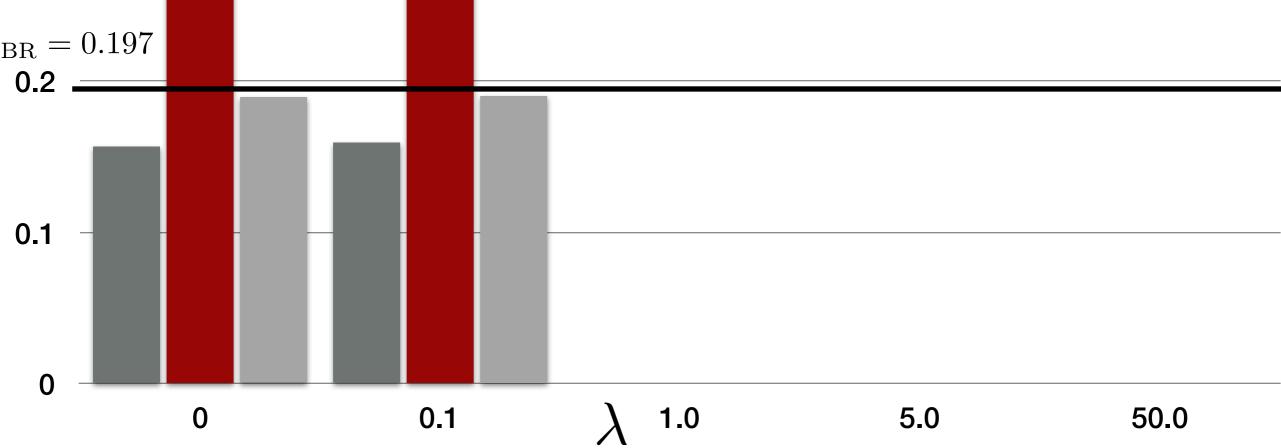
$$\Delta_{\mathrm{BR}} = 0.197$$
0.2

0.1

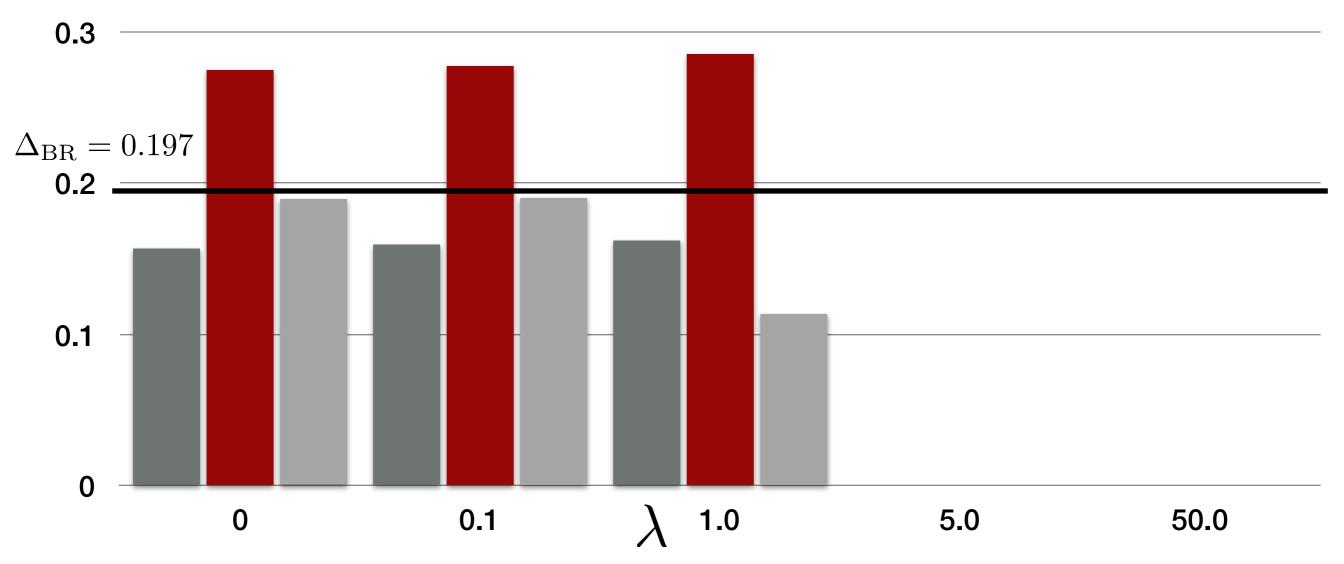
0 0.1
$$\lambda$$
 1.0 5.0 50.0



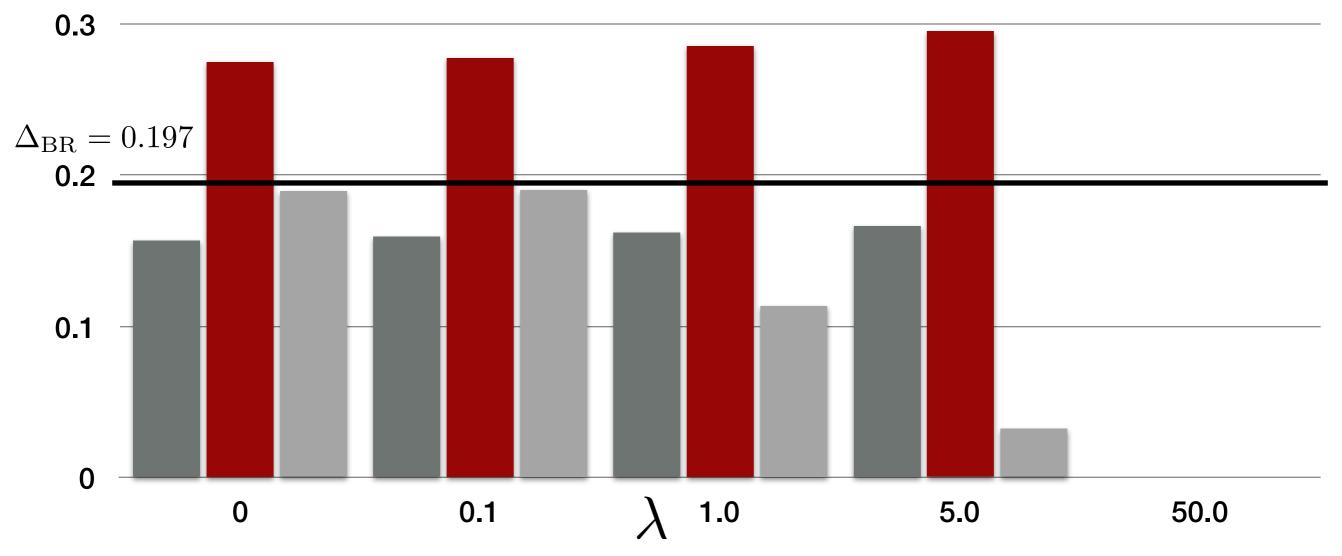


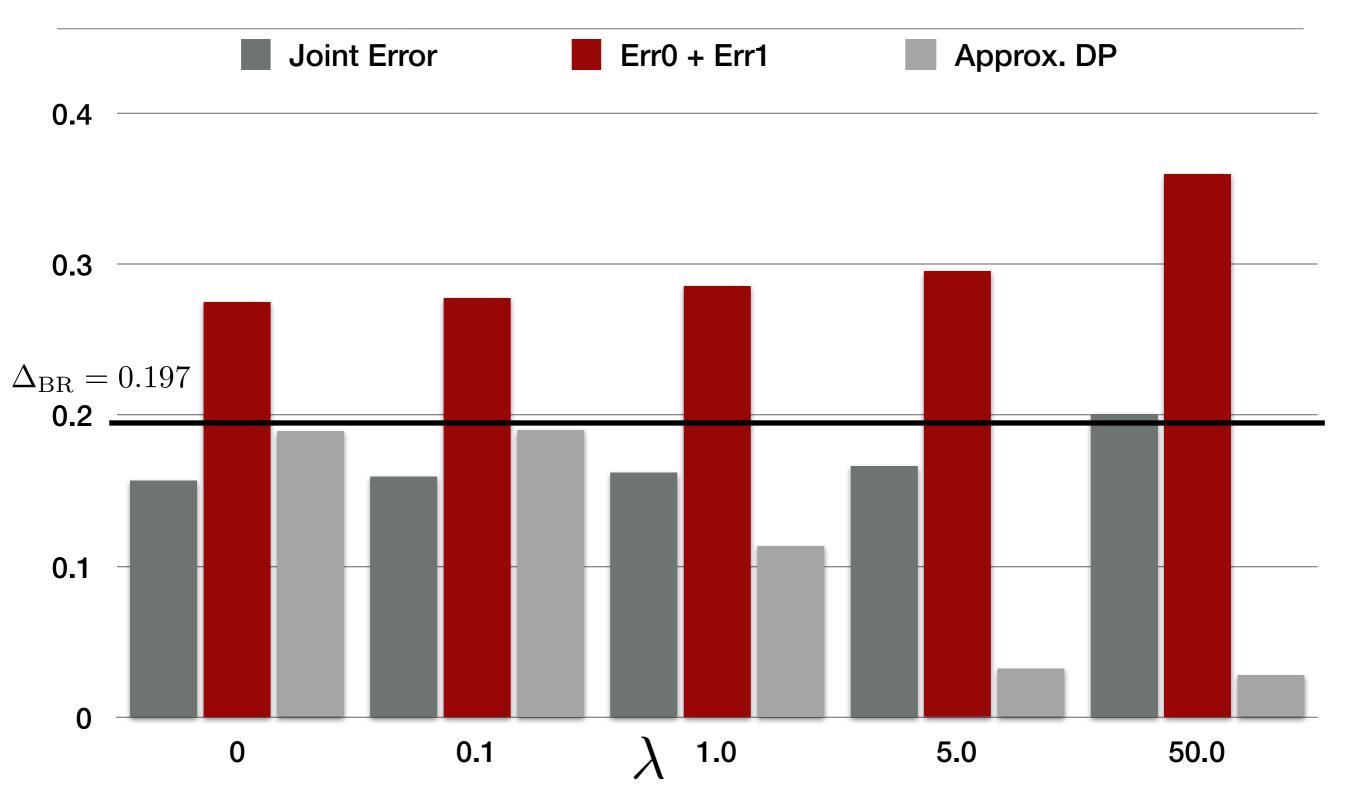












Thanks Q&A