Knowledge-based Security Policies

Joint work with Piotr Mardziel, Michael Hicks, and Mudhakar Srivatsa

Preserving Privacy

FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
	*** Totals ***		1,515.63	1,442.61	

Approach 1: Deny Access

FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

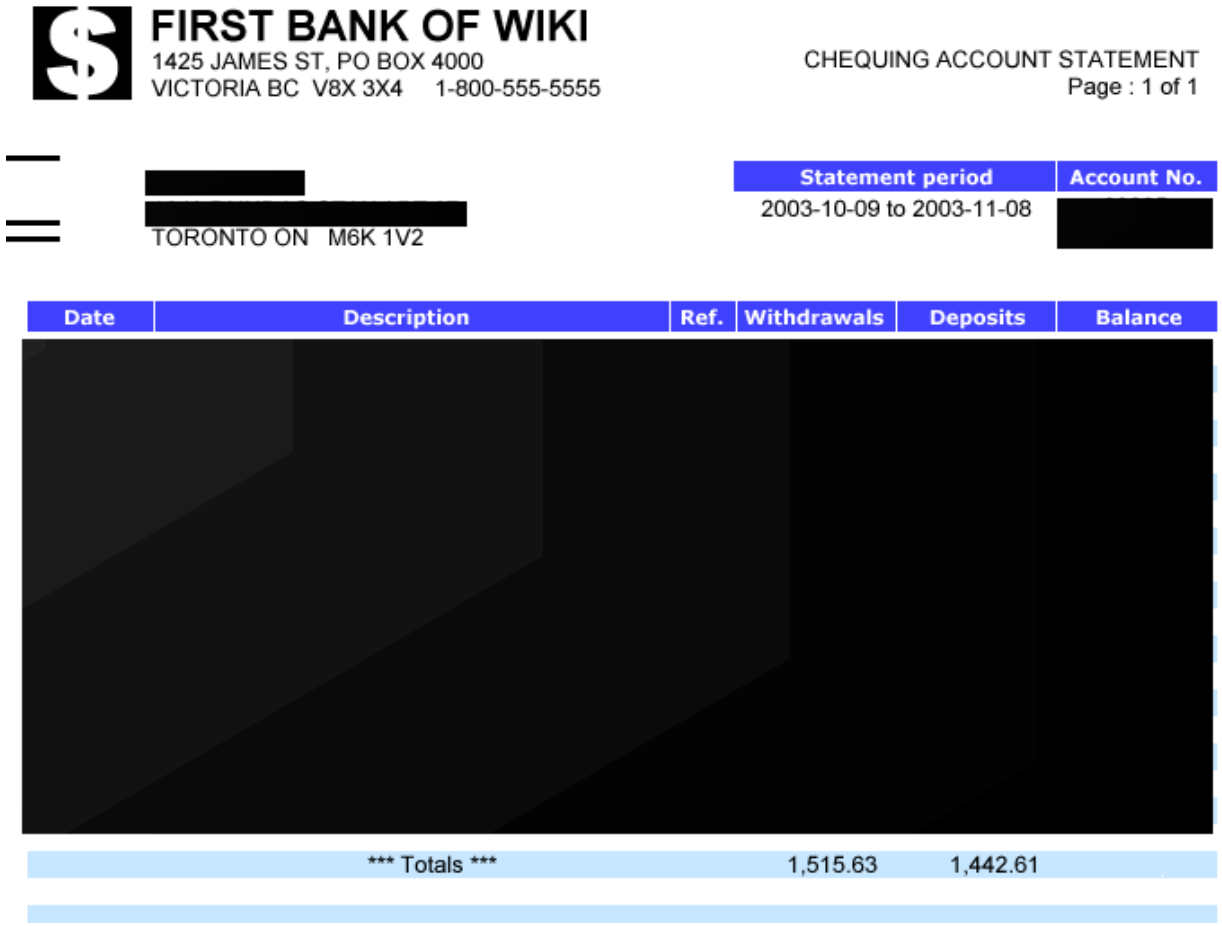
CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

JOHN JON
1643 DUND
TORONTO

nt period	Account No.
o 2003-11-08	00005- 123-456-7

Date			Deposits	Balance
2003-10-08	Previous			0.55
2003-10-14	Payroll D		694.81	695.36
2003-10-14	Web Bill			495.36
2003-10-16	ATM With			474.11
2003-10-16	Fees - Int	0		472.61
2003-10-20	Interac Pu	9		469.62
2003-10-21	Web Bill P	0		169.62
2003-10-22	ATM Witho	0		69.62
2003-10-23	Interac Pur	8		40.54
2003-10-24	Interac Ref		2.99	43.53
2003-10-27	Telephone	77		36.76
2003-10-28	Payroll Dep		694.81	731.57
2003-10-30	Web Funds		50.00	781.57
2003-11-03	Pre-Auth. Pay	55		748.02
2003-11-03	Cheque No. -	00		648.02
2003-11-06	Mortgage Paym	710.49		-62.47
2003-11-07	Fees - Overdra	5.00		-67.47
2003-11-08	Fees - Monthly	5.00		-72.47
	*** Totals ***	1,515.63	1,442.61	

Approach 2: Redaction



FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

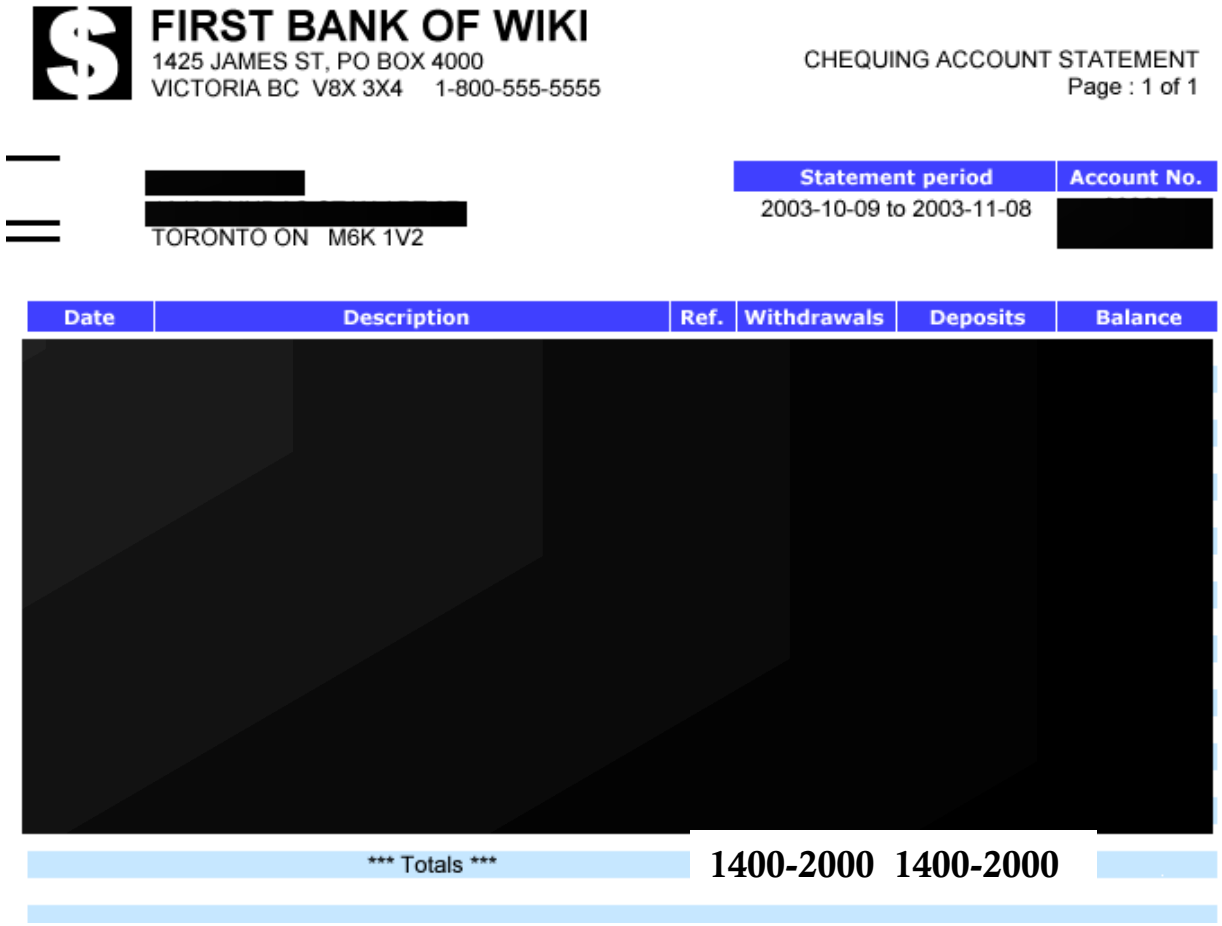
CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

[redacted]
[redacted]
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	[redacted]

Date	Description	Ref.	Withdrawals	Deposits	Balance
[redacted]					
	*** Totals ***		1,515.63	1,442.61	

Approach 3: Blurring



FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

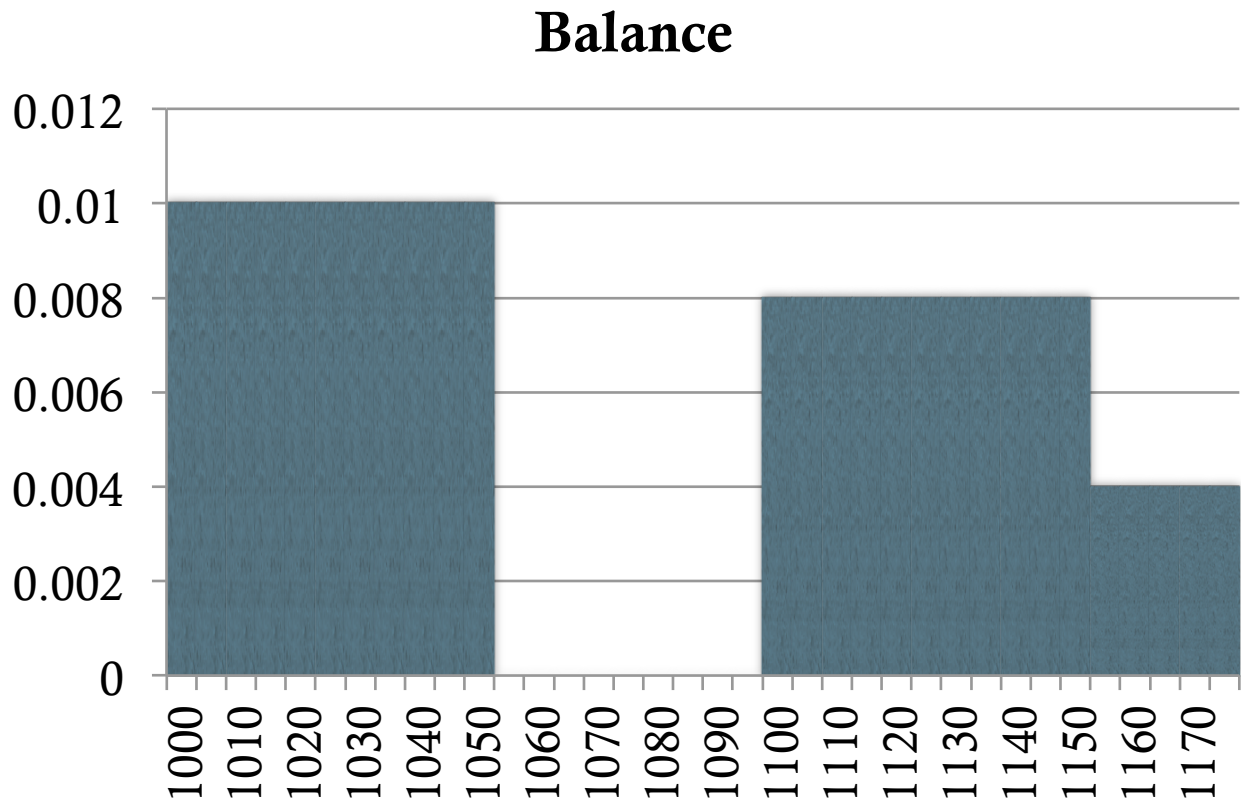
[redacted]
[redacted]
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	[redacted]

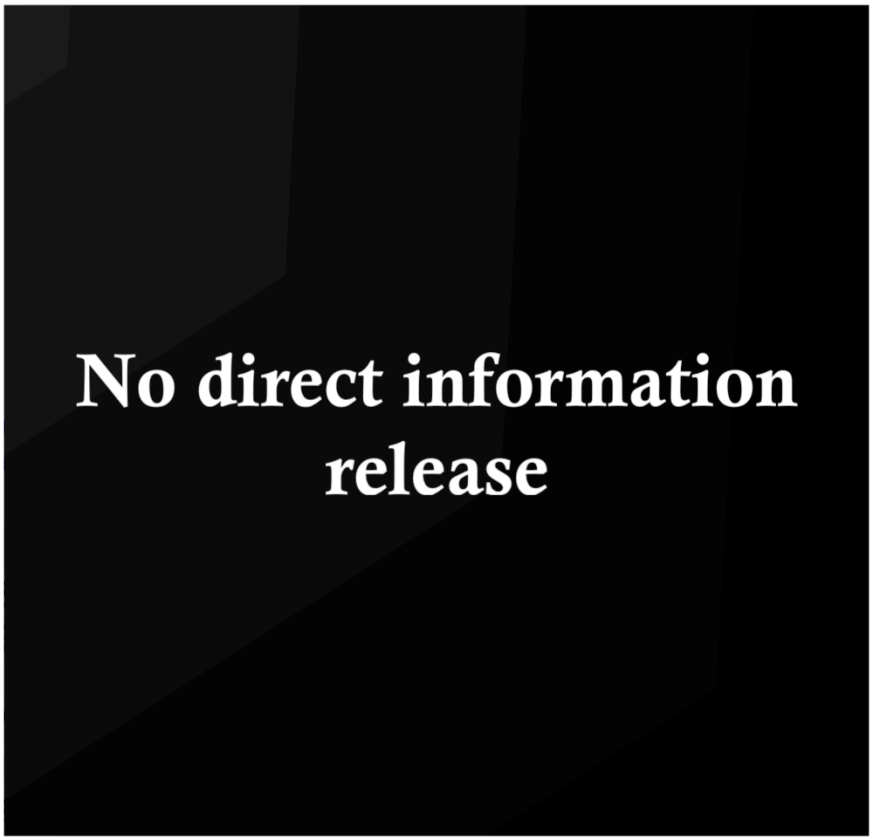
Date	Description	Ref.	Withdrawals	Deposits	Balance
[redacted]					
*** Totals ***			1400-2000	1400-2000	

Knowledge-Based Policy

- Cannot know exact dollar amount of any transaction with greater than 0.01% certainty.
  - Implies range of at least $100 (10k values)
- Cannot know exact balance amount with greater than 0.005% certainty.
  - Range of at least $200
- Also permits non-contiguous uncertainty
  - Balance $1,000 - $1,050 with 50% probability
  - Balance $1,100 - $1,150 with 40% probability
  - Balance $1,150 - $1,175 with 10% probability


Balance
0.012
0.01
0.008
0.006
0.004
0.002
0
1000
1010
1020
1030
1040
1050
1060
1070
1080
1090
1100
1110
1120
1130
1140
1150
1160
1170

Approach 3: Blurring



Question:

Are there any withdrawals over $500?

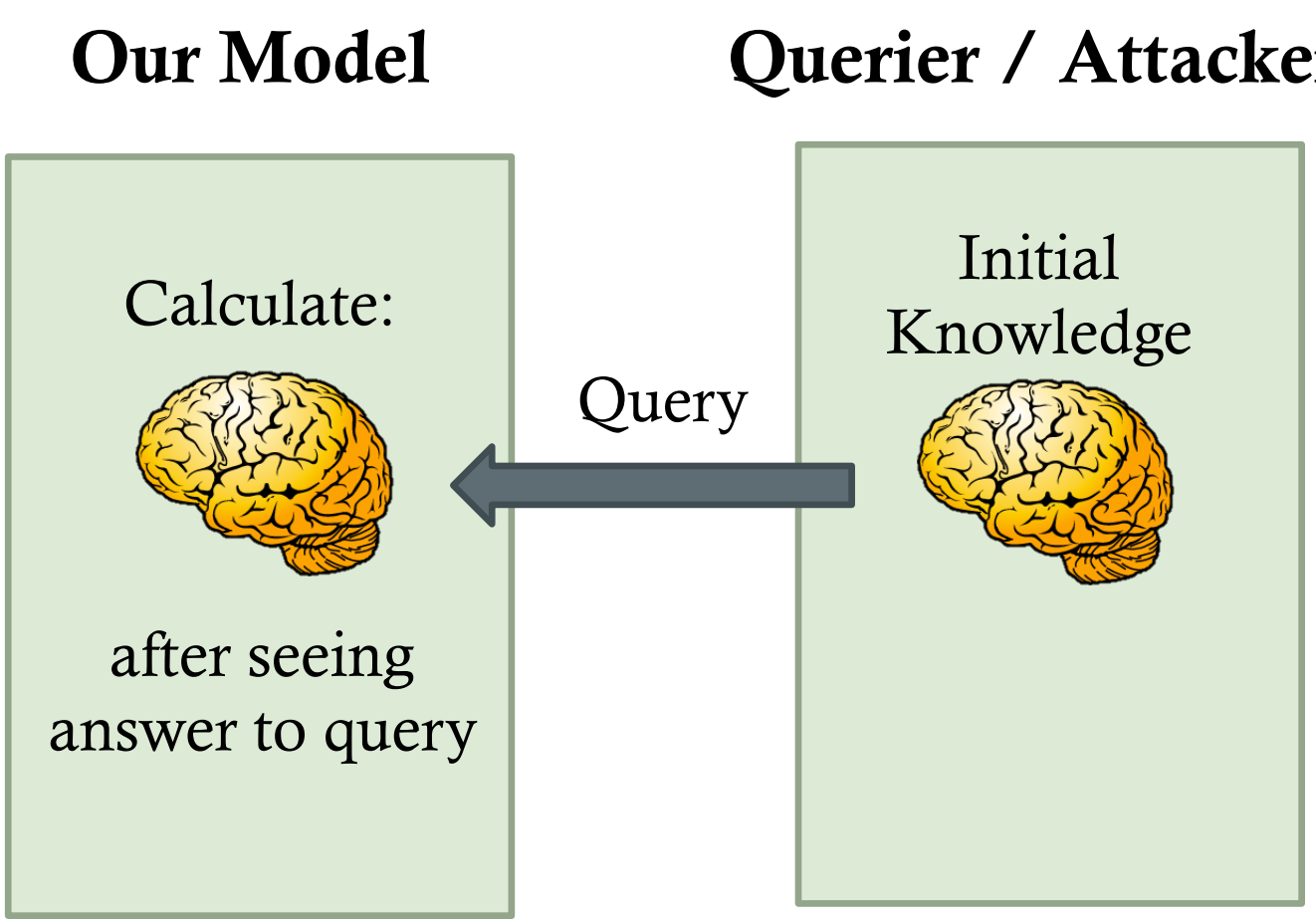
Can't answer this…

Goal: Answer as many questions as possible, while ensuring privacy bounds hold.

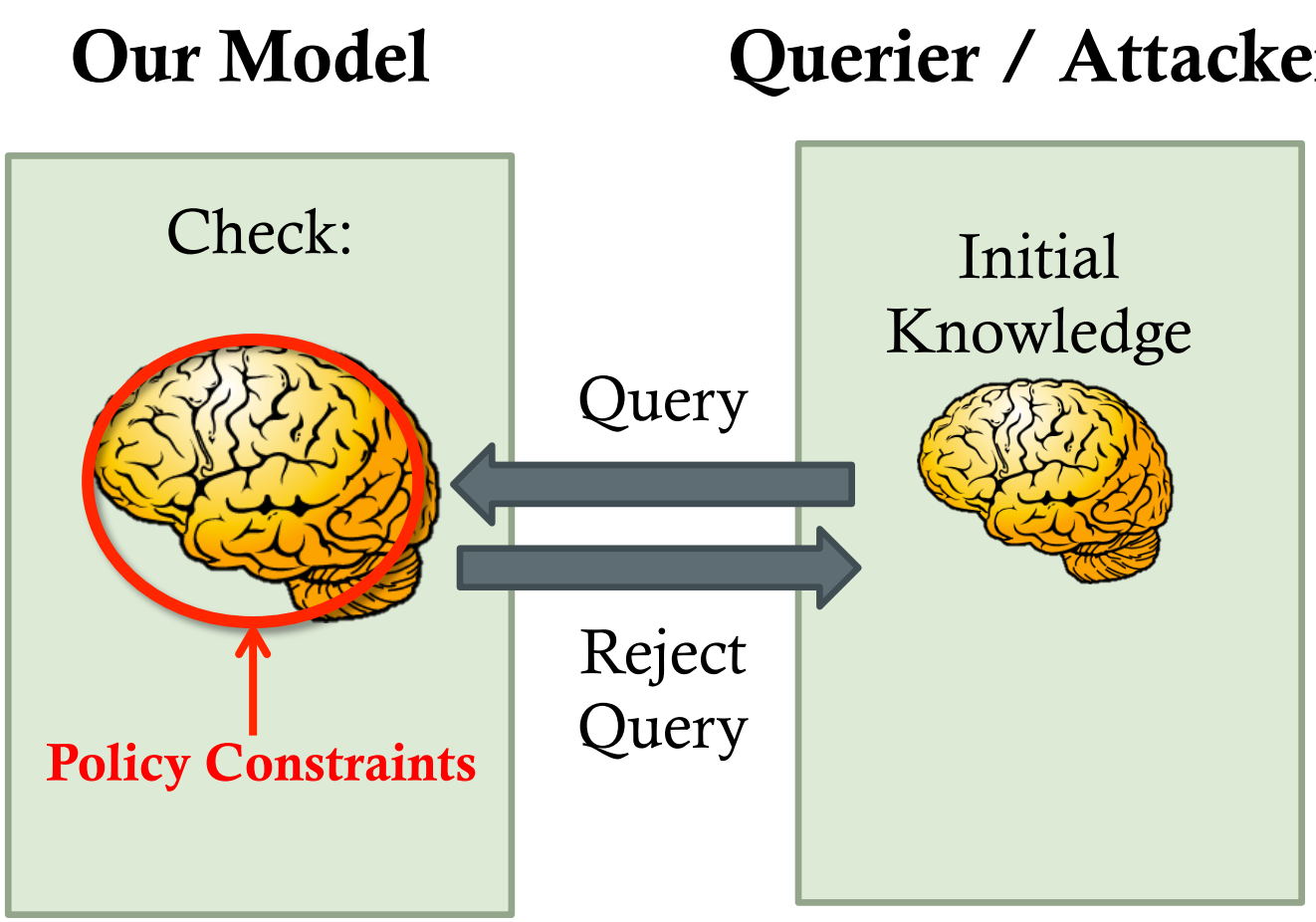
New Approach

- No a priori blurring or redaction
- Instead, selectively answer outside queries
  - Keep track of outsiders' knowledge
  - If answering query would reveal too much, don't answer
  - Otherwise, answer query and calculate the change in knowledge
- Always enforce knowledge-based policy
  - Cannot know exact dollar amount of any transaction with greater than 0.01% certainty.
  - Cannot know exact balance amount with greater than 0.005% certainty.

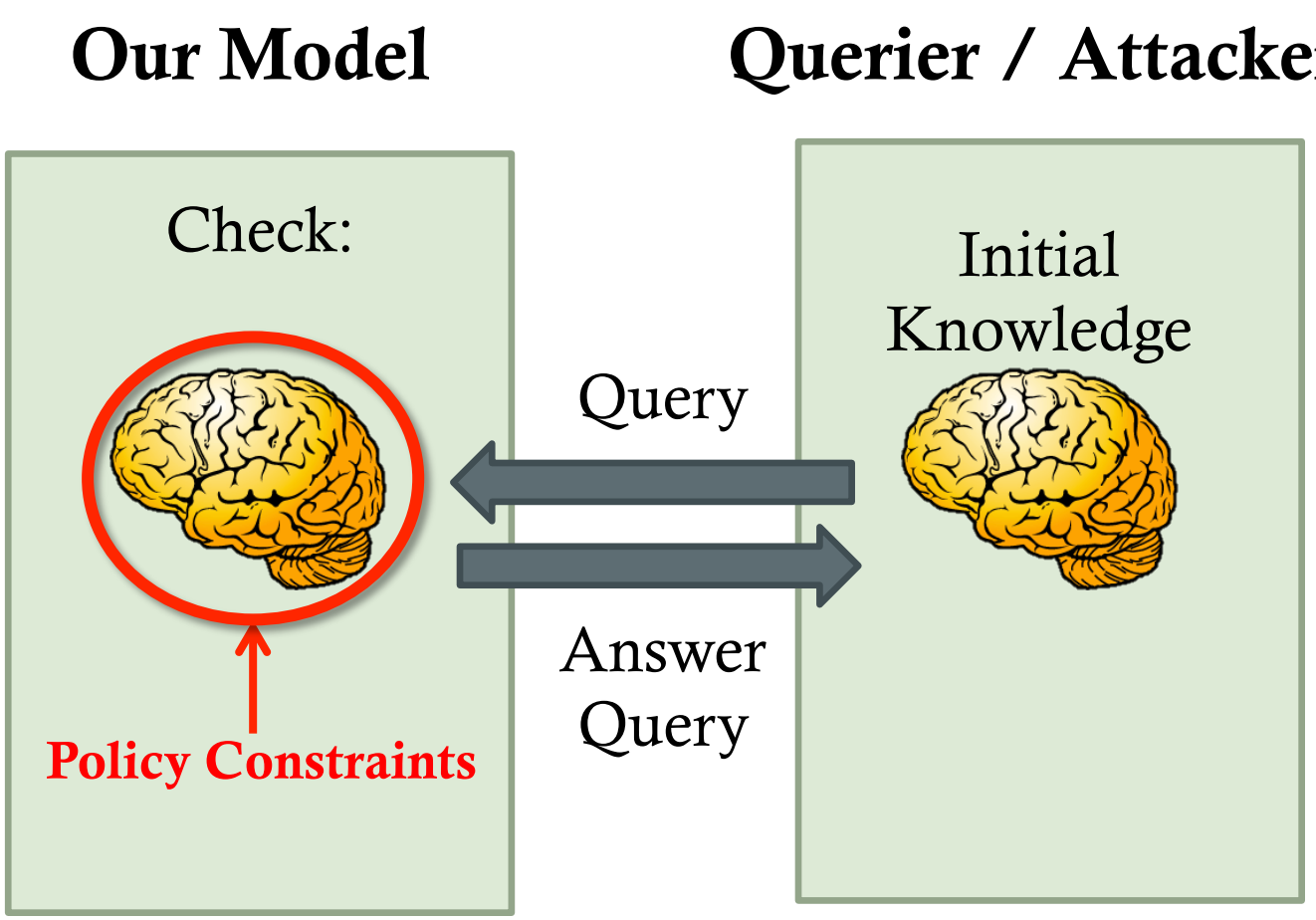
Policy Enforcement



Policy Enforcement

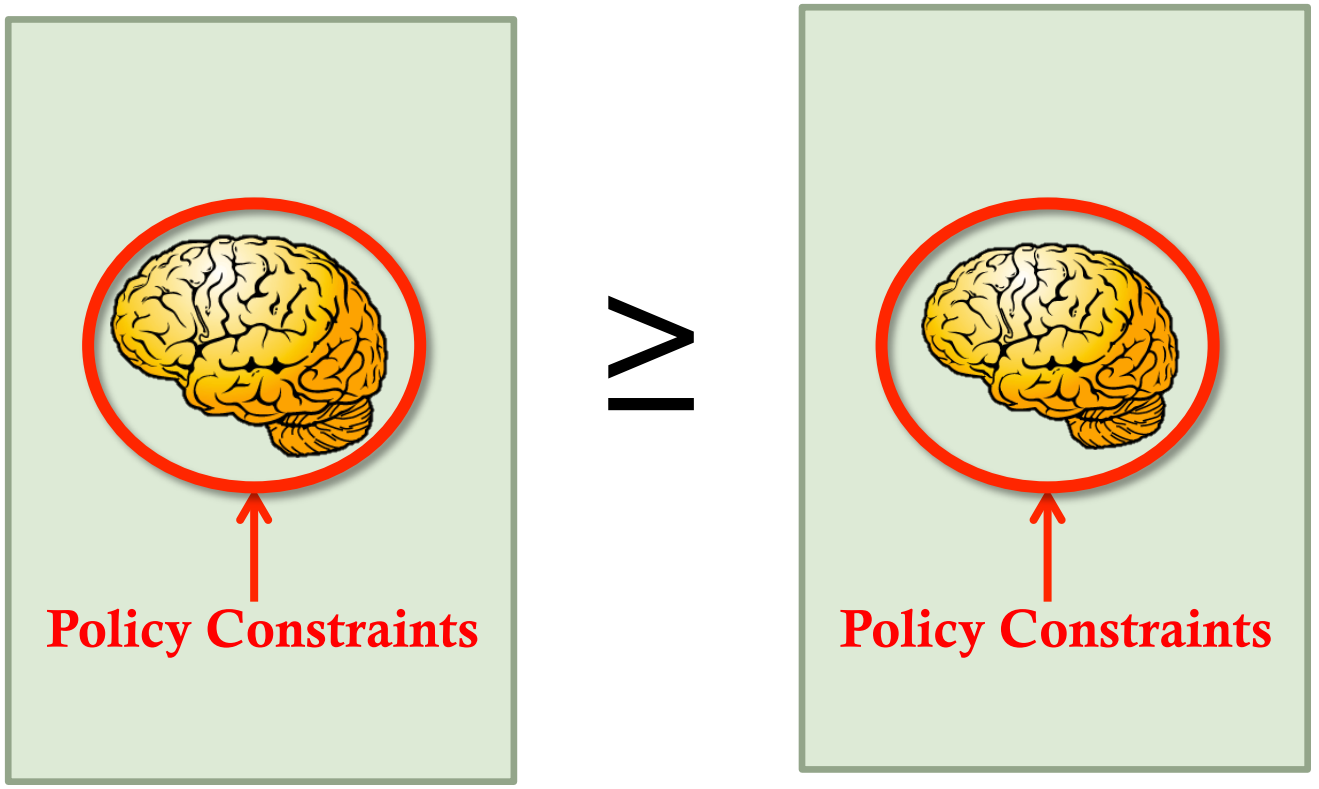


Policy Enforcement



Must Ensure…

Our Model ⊇ **Querier / Attacker**



Examples

- Bank Statements
  - **Lender**: Any withdrawals over $5k?
- Demographic Data
  - **Website**: Age between 24 – 30?
- Troop Deployments
  - **Coalition Partner**: Is allied support available within 1 hour of location X?
- Health Data
  - **Insurer**: Risk factors for heart disease?

the magic of macy's

free shipping every day of the year!
with $99 purchase. $8 Flat-Fee Shipping with purchases under $99. exclusions apply. details

shopping bag (0)
sign in | my account | customer service

for the home | bed & bath | women | men | juniors | kids | beauty & fragrance | shoes | handbags & accessories | jewelry & watches | sale

SEARCH Keyword, Web ID GO | the giftguide | STORES | DEALS & PROMOTIONS | GIFT CARDS | WEDDING REGISTRY

DKNY
View All Men's

Narrow by

Size Family

S	M	L	XL
2XL	29	30	31
32	33	34	36
38	39	40	41
42	44	46	48
OS			

Color Family

Customers Top Rated
★★★★★ 5 stars (5)
★★★★☆ 4 stars & up (15)
★★★☆☆ 3 stars & up (16)

Price
Under $50 (31)
$50-$100 (29)
$100-$250 (3)
$250-$500 (7)
$500 & Above (3)
$ min to $ max Go

70 items in DKNY

Sort by: Featured Items Show: 40 items Page **1** 2 Next

NEW! DKNY Jeans, Medium Wash Bleecker Fit
$59.50

MORE COLORS AVAILABLE
NEW! DKNY Tie, Skinny Stella Stripe
$59.50

DKNY Jeans Shirt, Crinkle Plaid
$69.50

DKNY Dress Shirt, Fitted Pale Pink Solid
Reg. $65.00
Sale $46.99

DKNY Dress Shirt, Fitted Bermuda Stripe
$65.00

MORE COLORS AVAILABLE
DKNY Jeans Shorts, Solid Cargo Shorts
$49.50

NEW! DKNY Jeans Shirt, Short Sleeved Crinkle Plaid Shirt
$59.50

NEW! DKNY Jeans Shirt, Ikat Plaid Shirt
$69.50

the magic of macy's

free shipping every day of the year!
with $99 purchase. $8 Flat-Fee Shipping with purchases under $99. exclusions apply. details

shopping bag (0)
sign in | my account | customer service

for the home | bed & bath | women | men | juniors | kids | beauty & fragrance | shoes | handbags & accessories | jewelry & watches | sale

SEARCH Keyword, Web ID GO | the giftguide | STORES | DEALS & PROMOTIONS | GIFT CARDS | WEDDING REGISTRY

Donald J Trump

View All Men's

Dress Shirts
Ties
Accessories

Narrow by

Size Family

38 | 40 | 42 | 44 | OS

Color Family

Customers Top Rated

★★★★★ 5 stars (11)
★★★★☆ 4 stars & up (14)
★★★☆☆ 3 stars & up (14)

Price

Under $20 (0)
$20-$40 (11)
$40-$60 (14)
$60-$80 (6)
$80-$100 (0)
$100 & Above (1)

$ min to $ max Go

32 items in Donald J Trump

Sort by: Featured Items Show: 40 items Showing All 32 Items

MORE COLORS AVAILABLE
NEW! Donald Trump Tie, Natte Stripe Silk Tie
$59.50

NEW! Donald Trump Shirt, Striped Long Sleeved Dress Shirt
$69.50

NEW! Donald Trump Shirt, French Cuff Solid Long Sleeve Dress Shirt
$69.50

MORE COLORS AVAILABLE
Donald Trump Tie, Falcon Metallic Stripe
Reg. $59.50
Sale $37.99

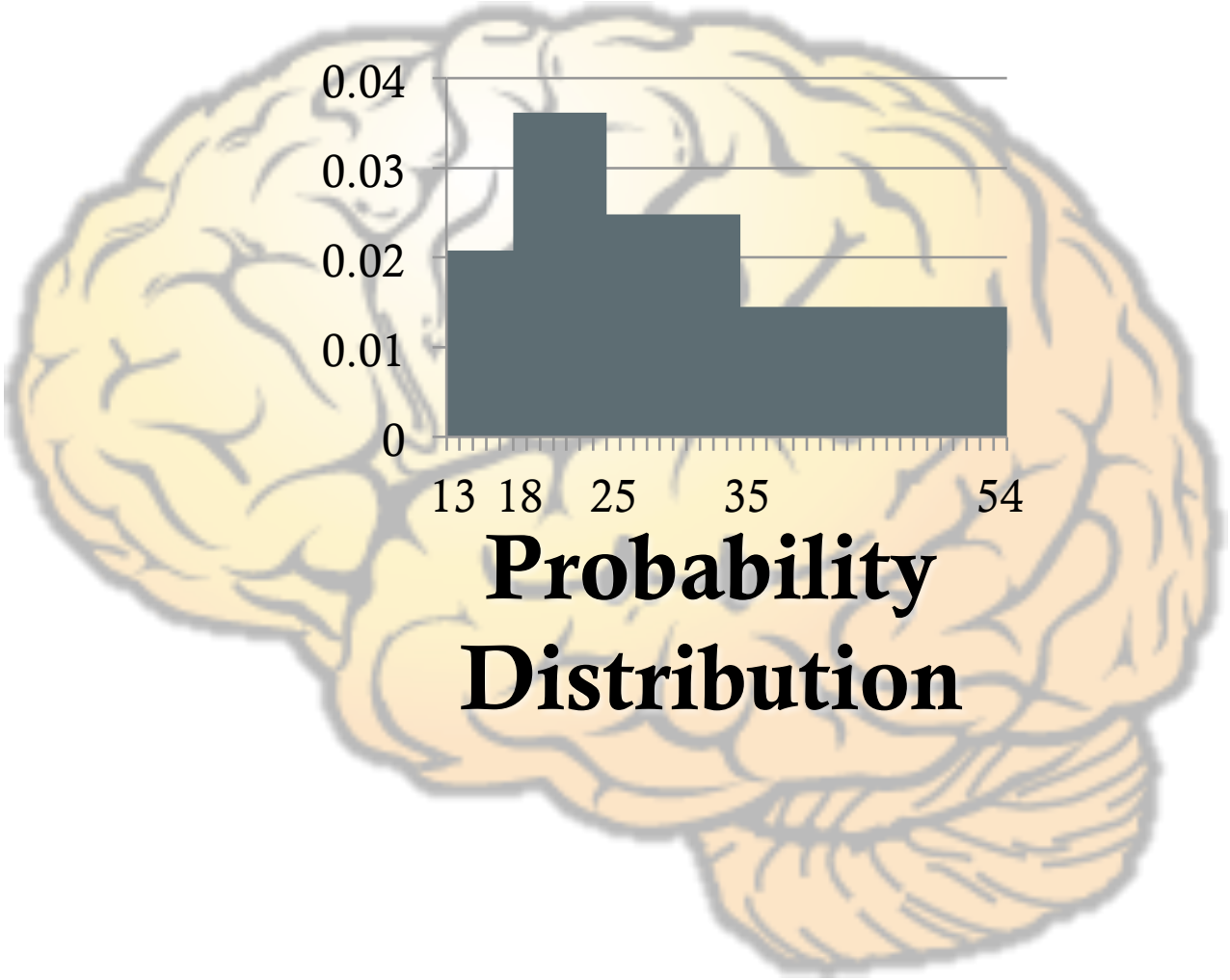
Donald Trump Dress Shirt, Non Iron White Blue Check
$69.50

Donald Trump Dress Shirt, Non Iron White Blue Stripe French Cuff
Reg. $69.50
Sale $46.99

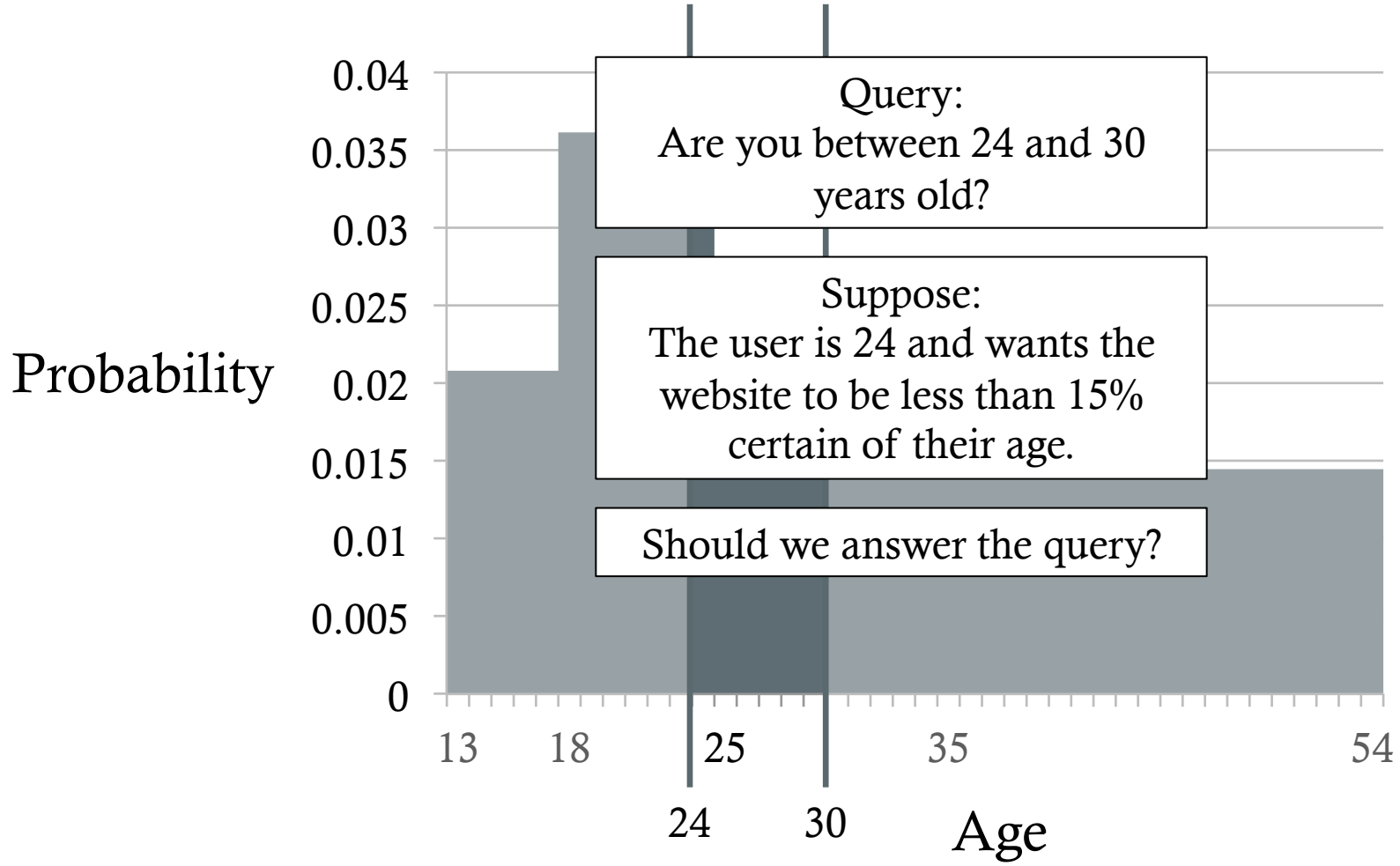
MORE COLORS AVAILABLE
Donald Trump Tie, Paisley
$59.50

Donald Trump Cufflinks, Polished Silver
$32.00

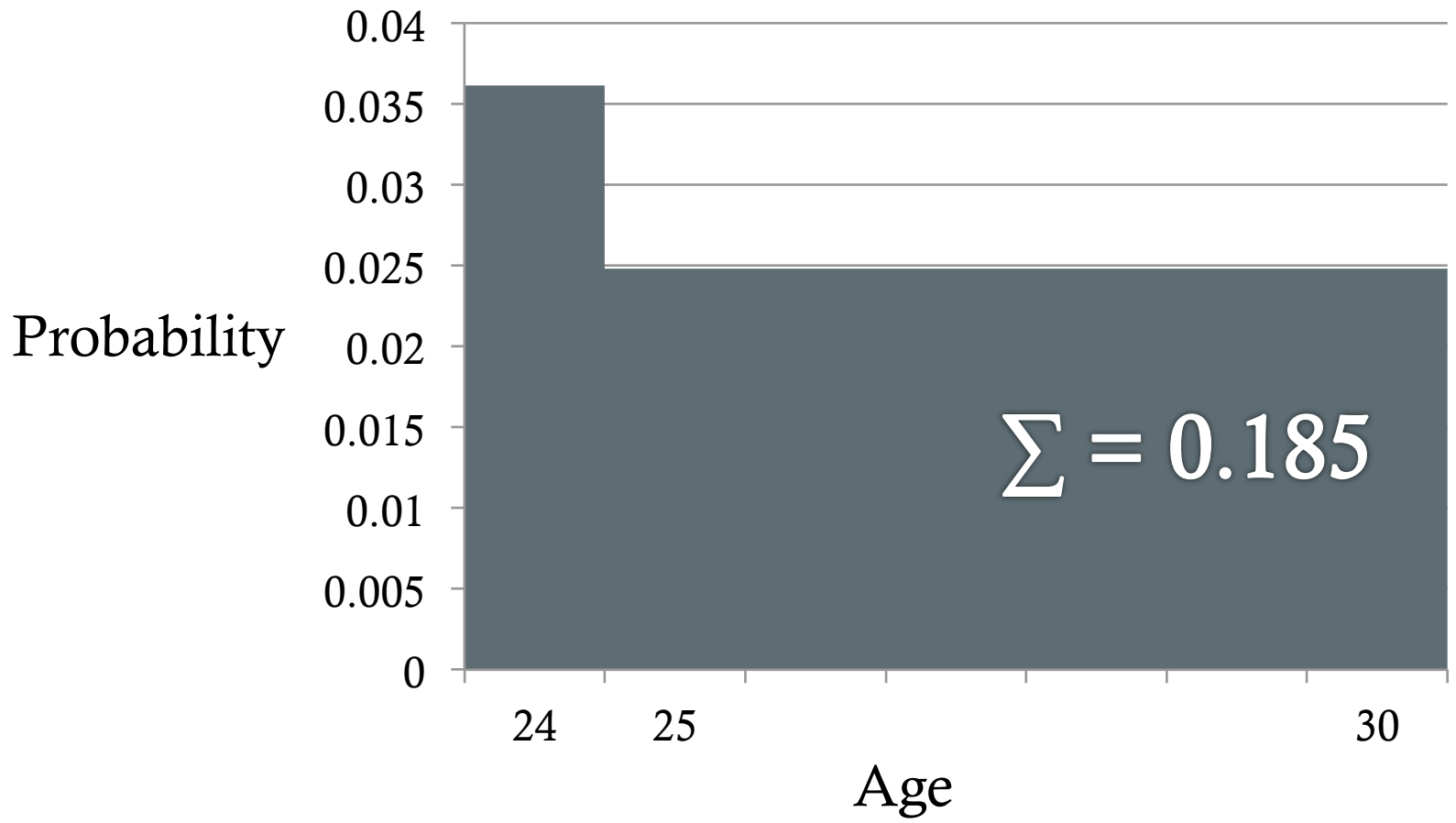
Modeling Knowledge



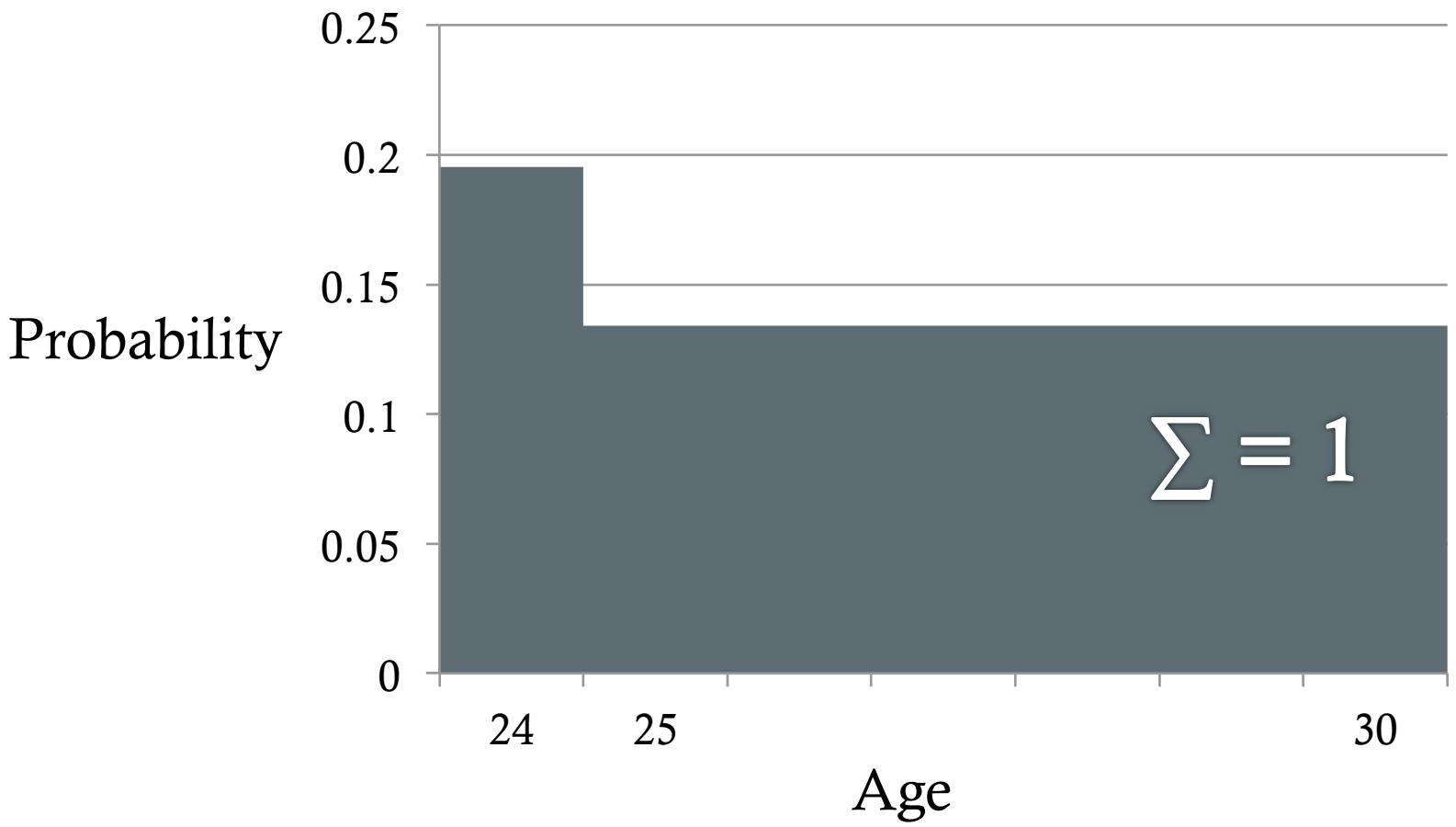
Modeling Beliefs



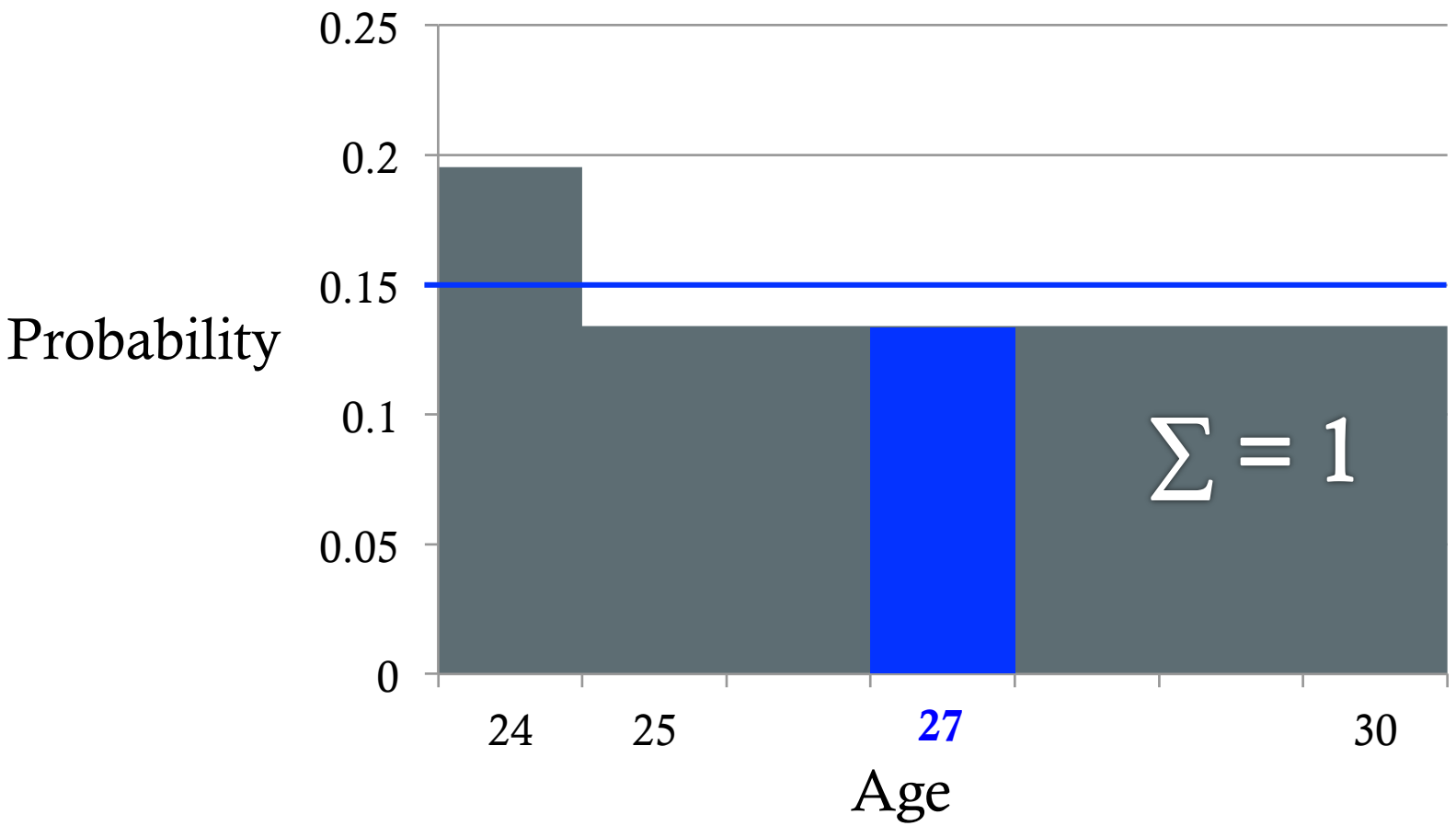
Modeling Beliefs



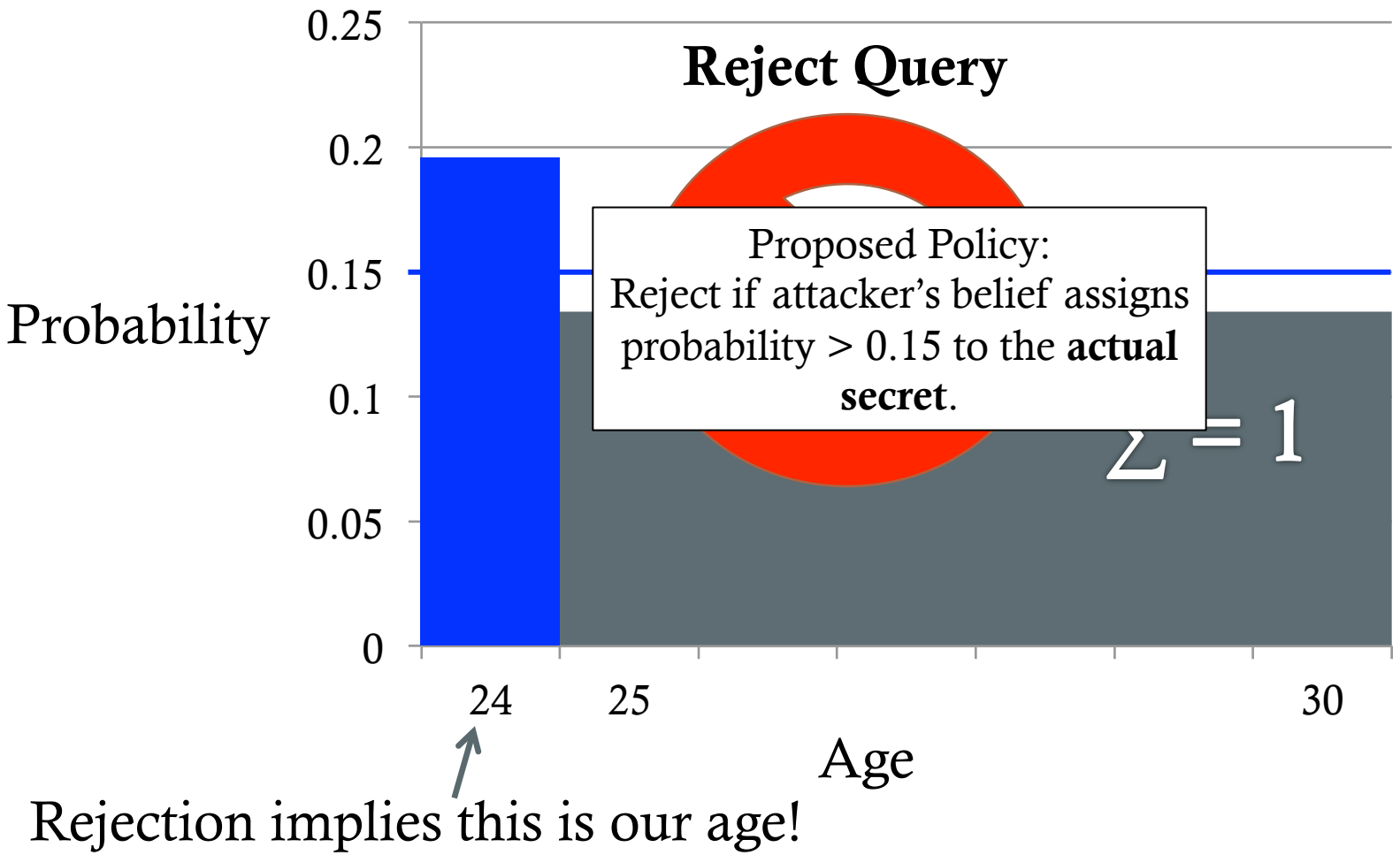
Modeling Beliefs



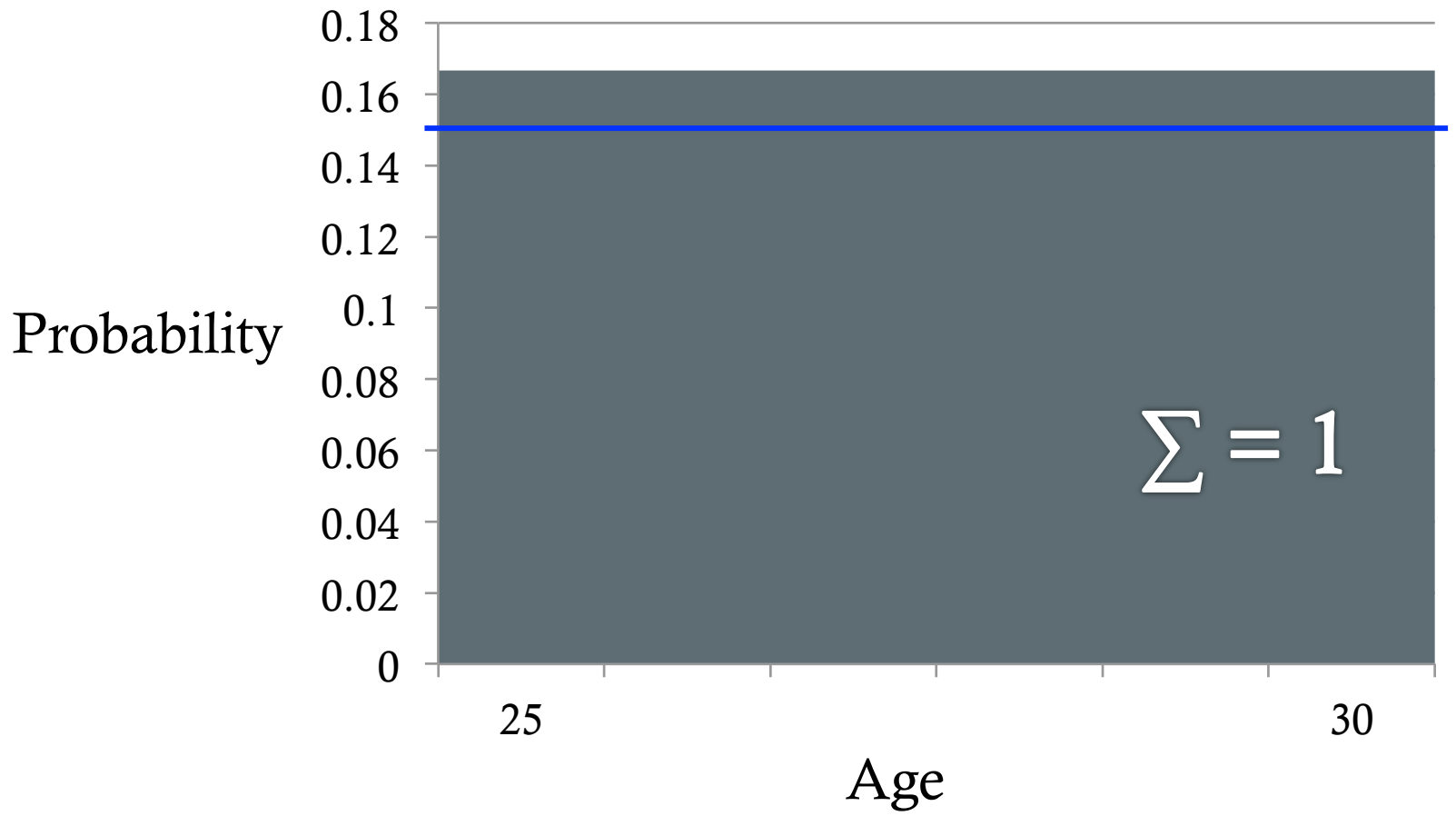
Modeling Beliefs



Modeling Beliefs



Modeling Beliefs

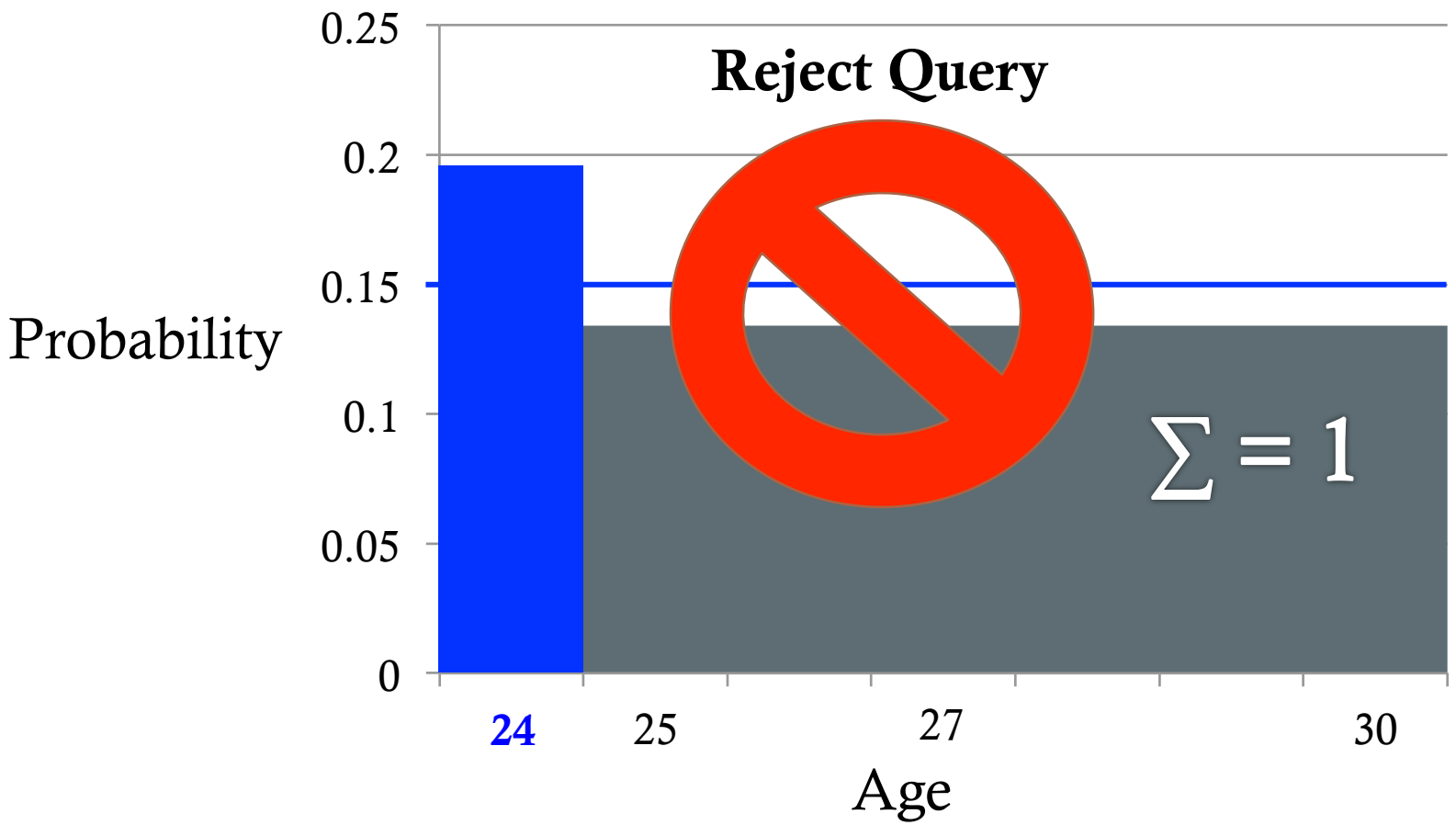


Problem:
Rejection could reveal information

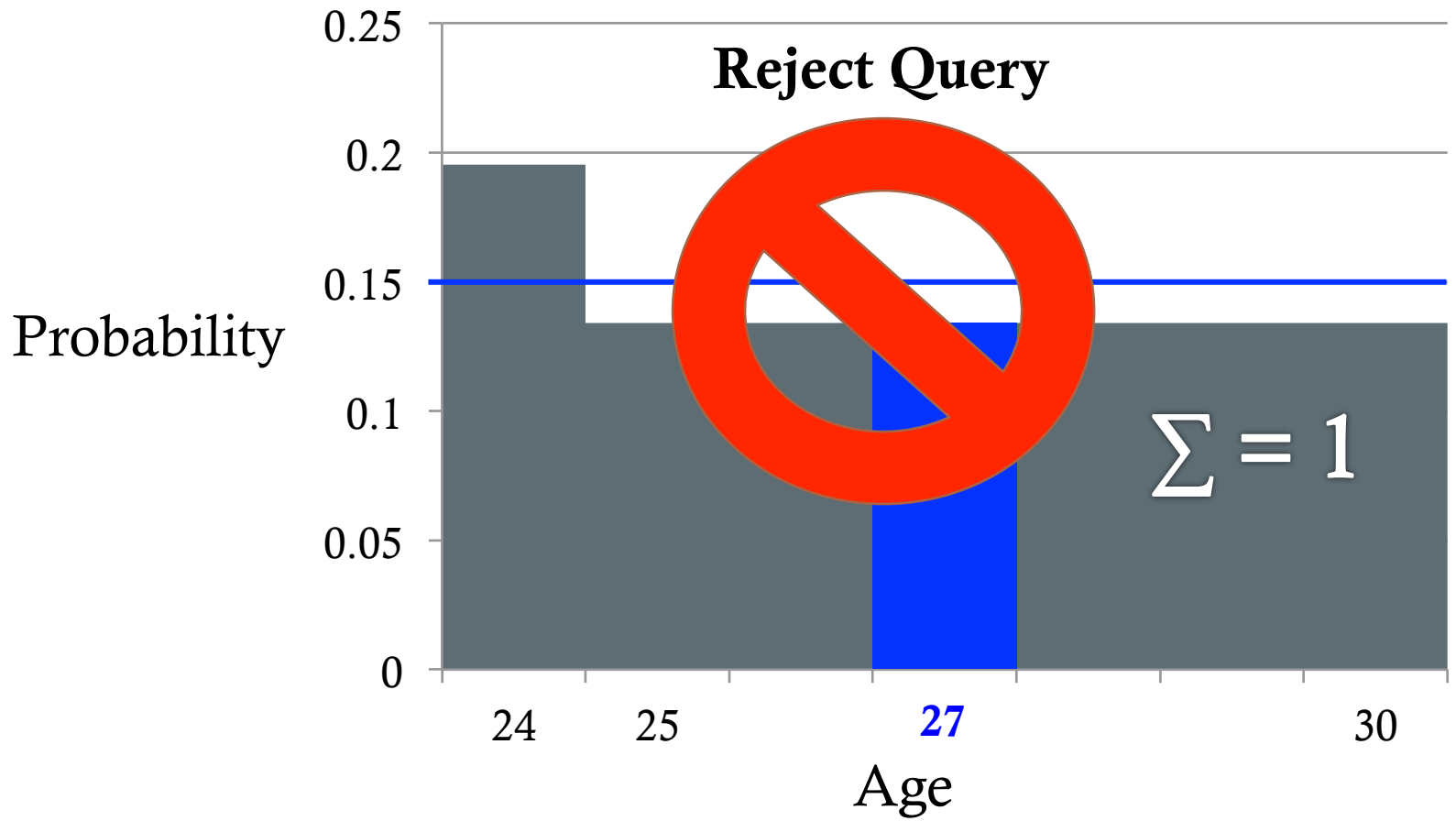
Solution:

Check that constraints are not violated ***for any possible secret***.

Modeling Beliefs



Modeling Beliefs



So Far…

- Mechanism for representing knowledge
  - Probability Distributions[1]
- Method for ensuring rejection does not leak information.
  - Check privacy for **all** possible secrets.
- One more issue… Efficiency!

[1] **Clarkson, Myers, Schneider**. "Quantifying Information Flow with Beliefs," Journal of Computer Security, 2009.

Problem

For large state spaces,

and complex sequences of queries

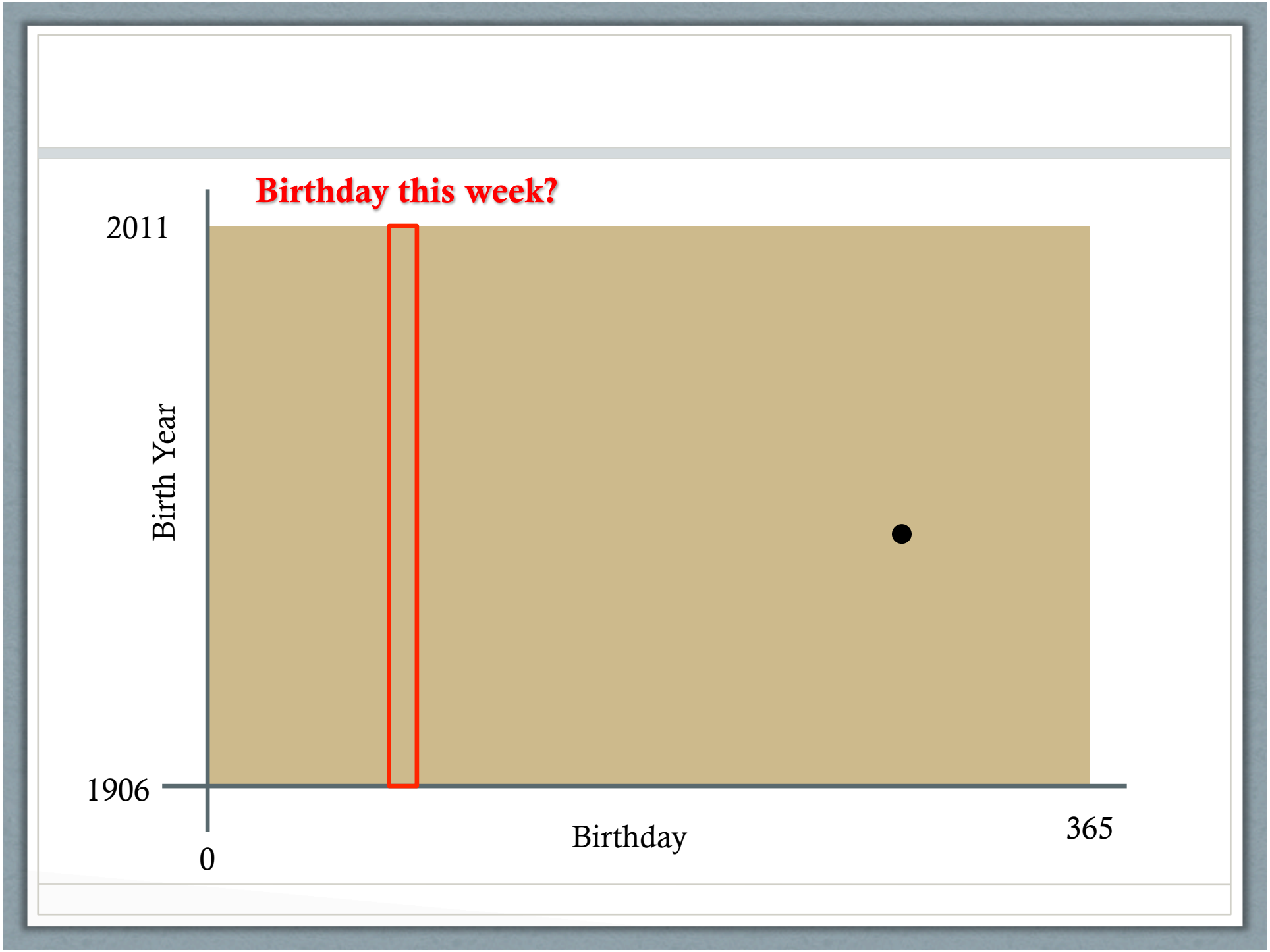
precise tracking is impractical.

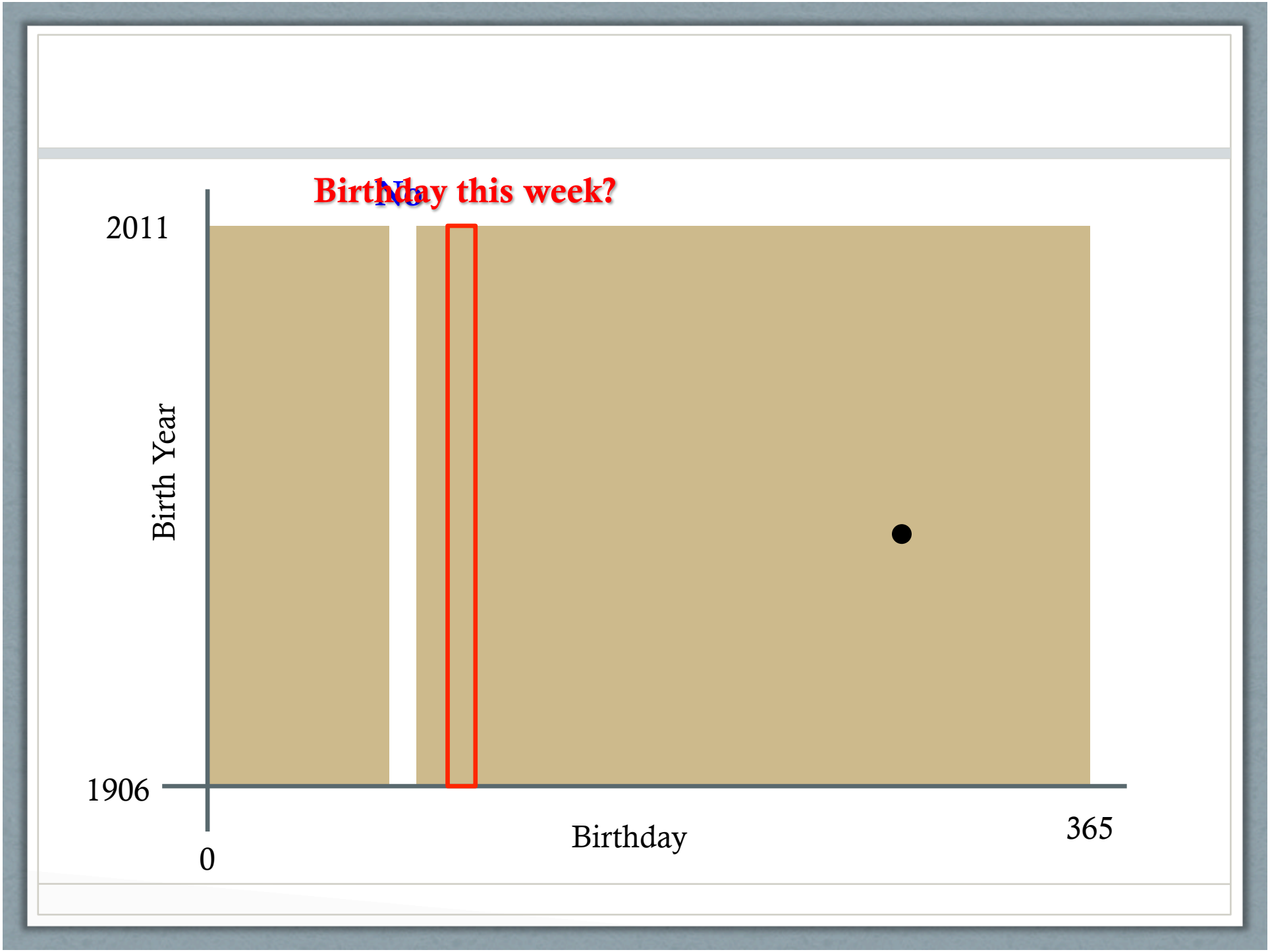
Birthday Query

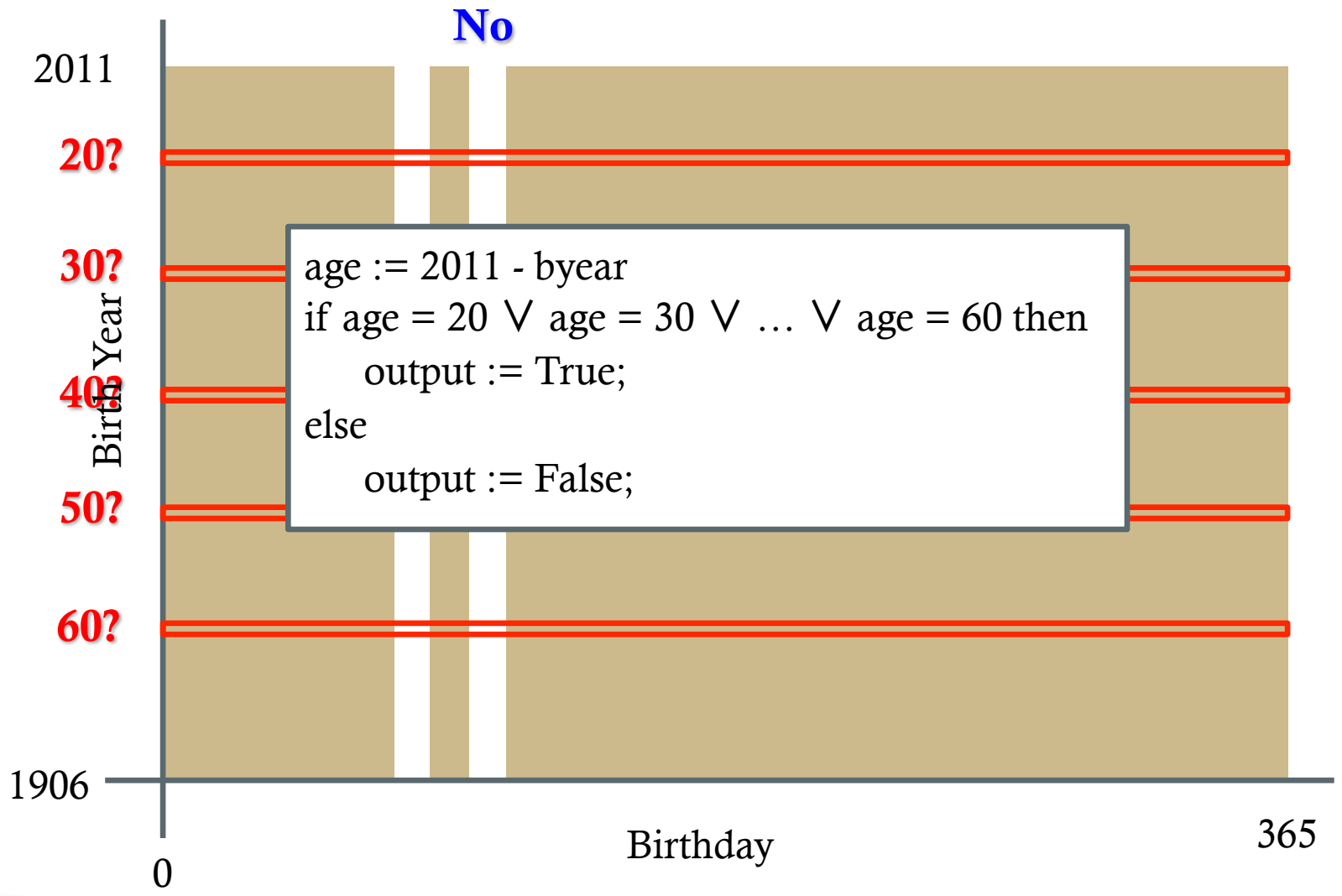
Birthday (bday) $\in$ [0,365]

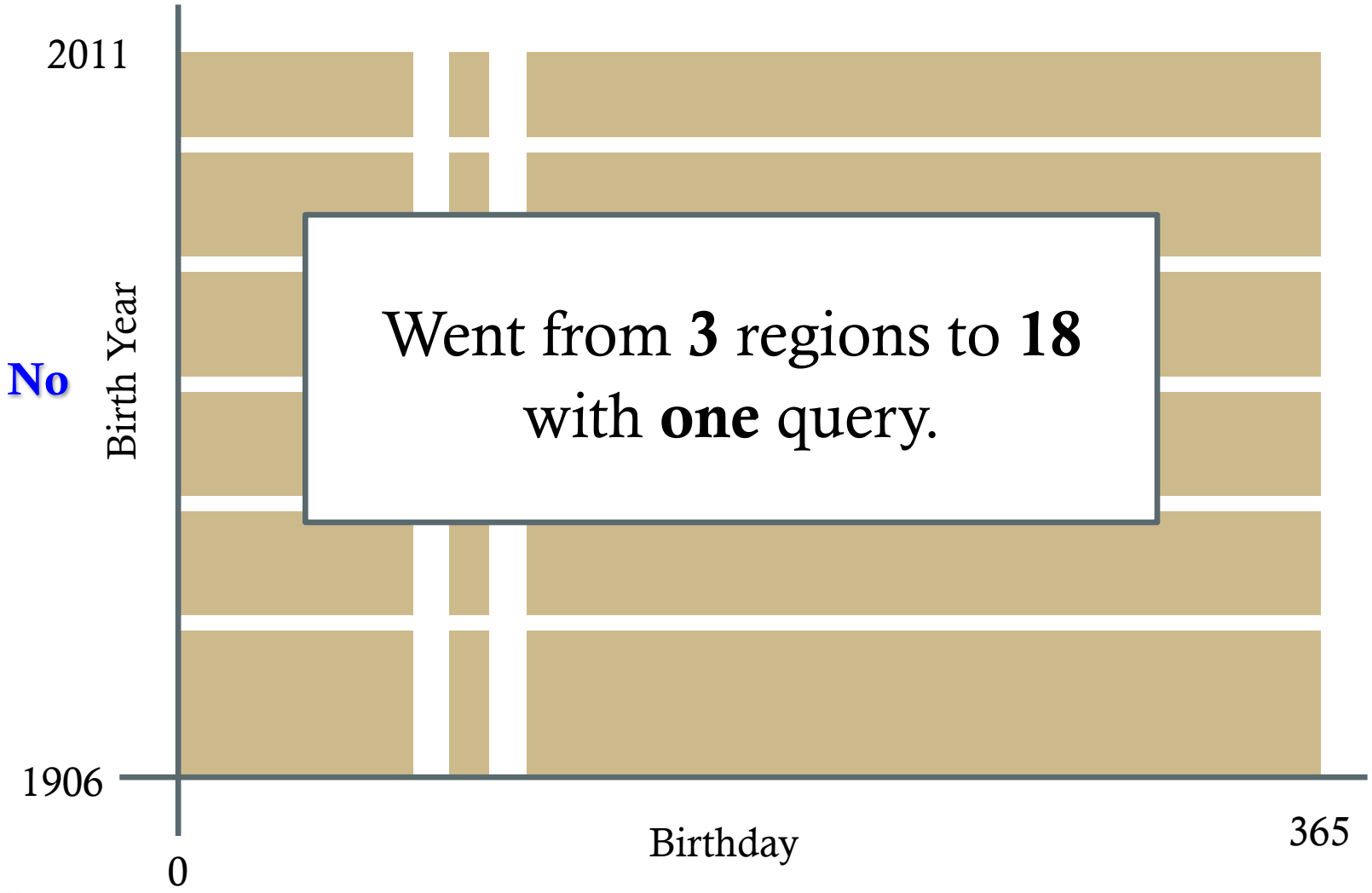
Birth Year (byear) $\in$ [1906, 2011]

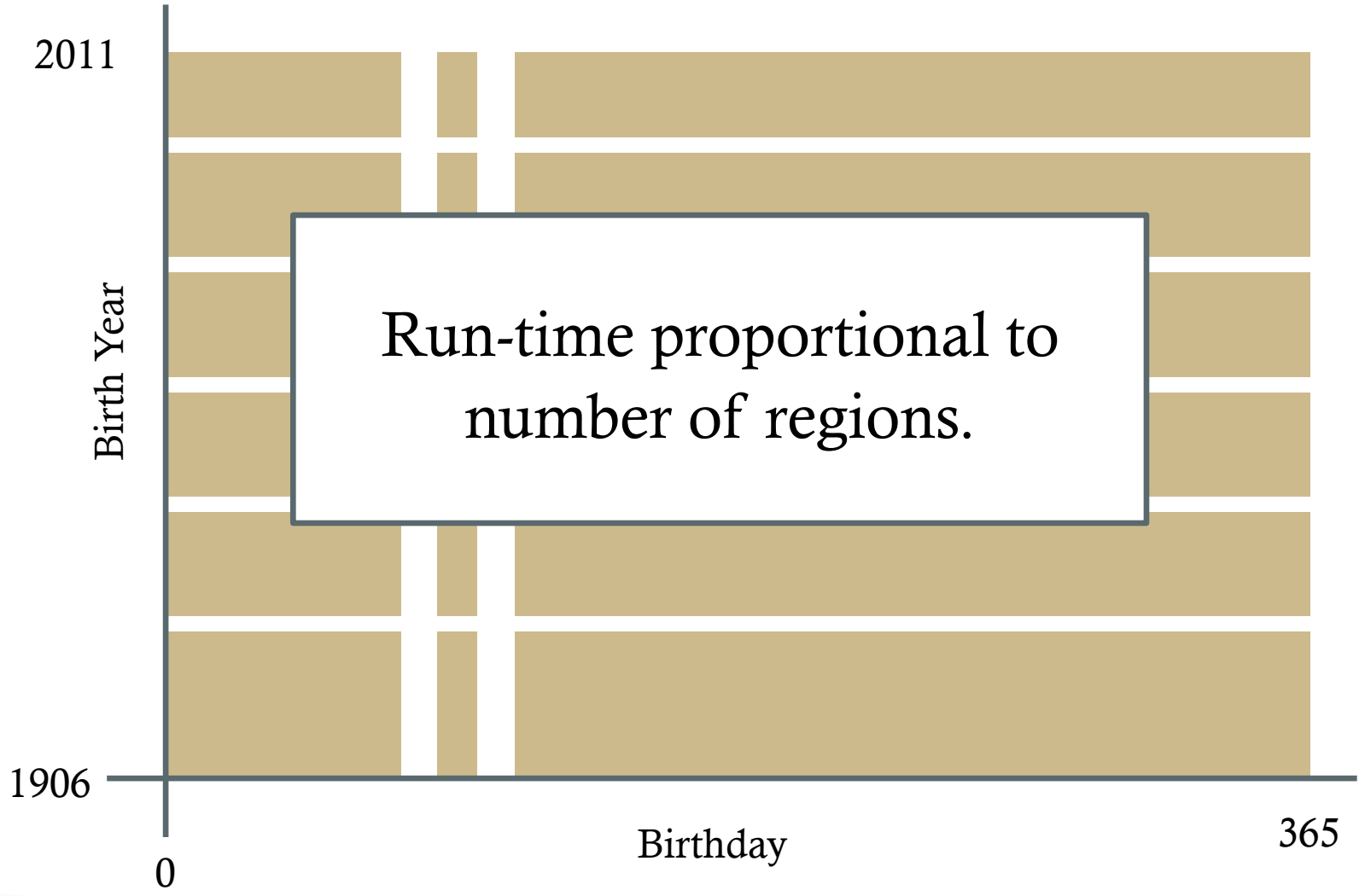
```
today := 260
if bday ≥ today ∧ bday < (today + 7) then
    output := True;
else
    output := False;
```

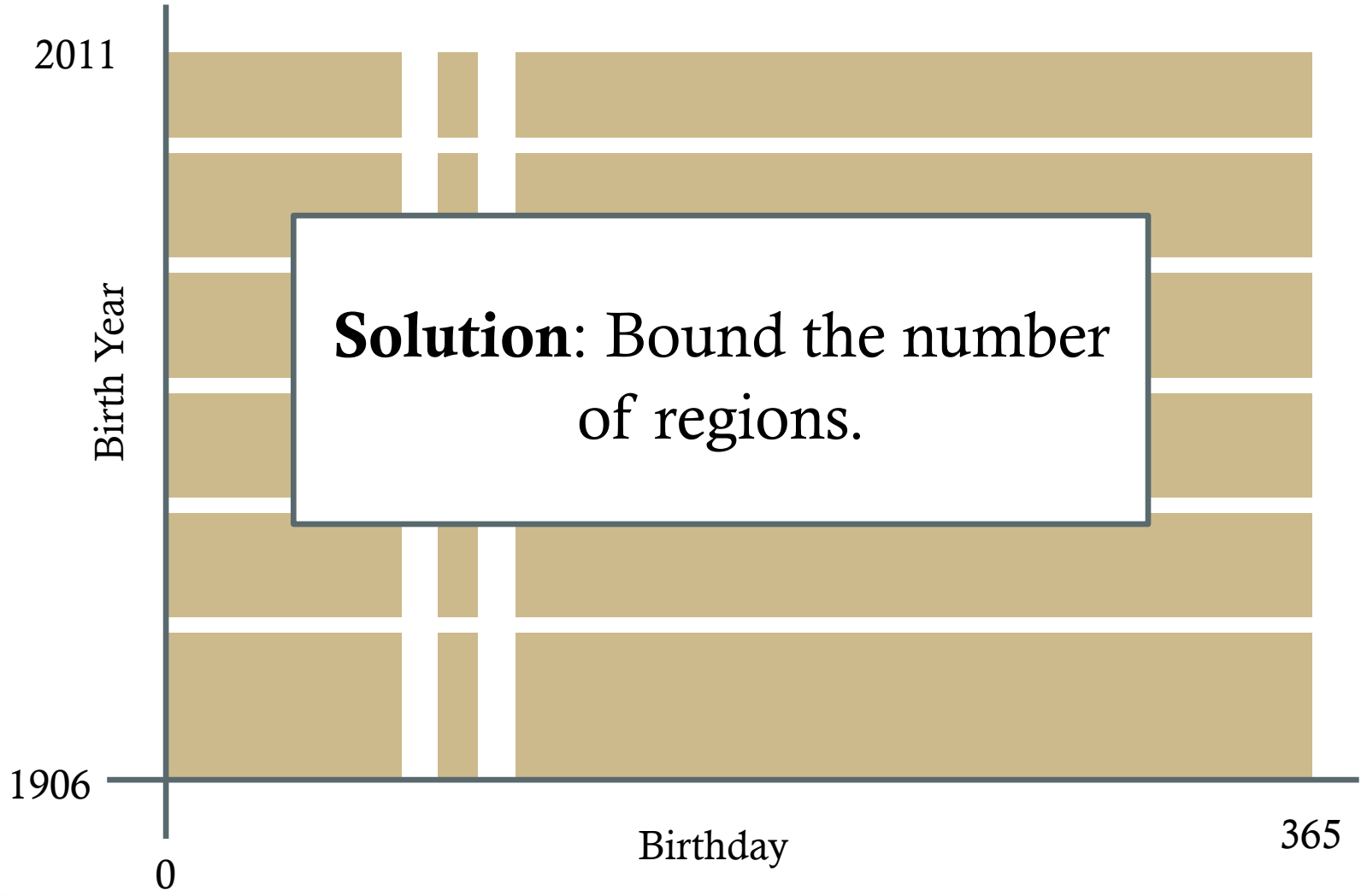

Birthday this week?
2011
Birth Year
1906
0
Birthday
365


Birthday this week?
No
2011
Birth Year
1906
0
Birthday
365


No
2011
20?
30?
40?
50?
60?
Birth Year
1906
0
Birthday
365
age := 2011 - byear
if age = 20 ∨ age = 30 ∨ … ∨ age = 60 then
output := True;
else
output := False;


2011
Birth Year
No
1906
0
Birthday
365
Went from **3** regions to **18** with **one** query.


2011
Birth Year
1906
0
Birthday
365
Run-time proportional to number of regions.


2011
Birth Year
1906
0
Birthday
365
Solution: Bound the number of regions.

Abstraction

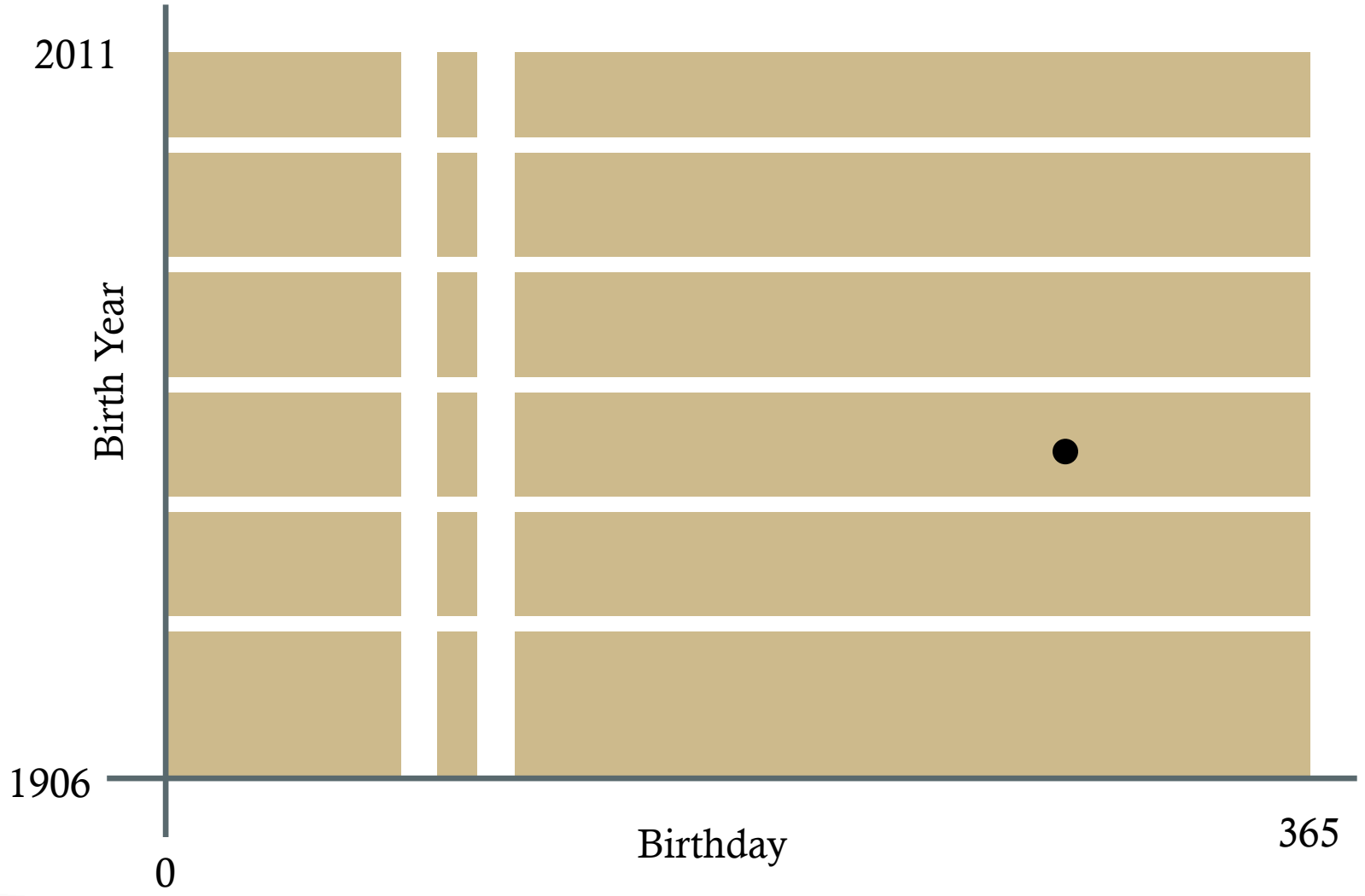
With bounded number of regions,

we can no longer be precise.

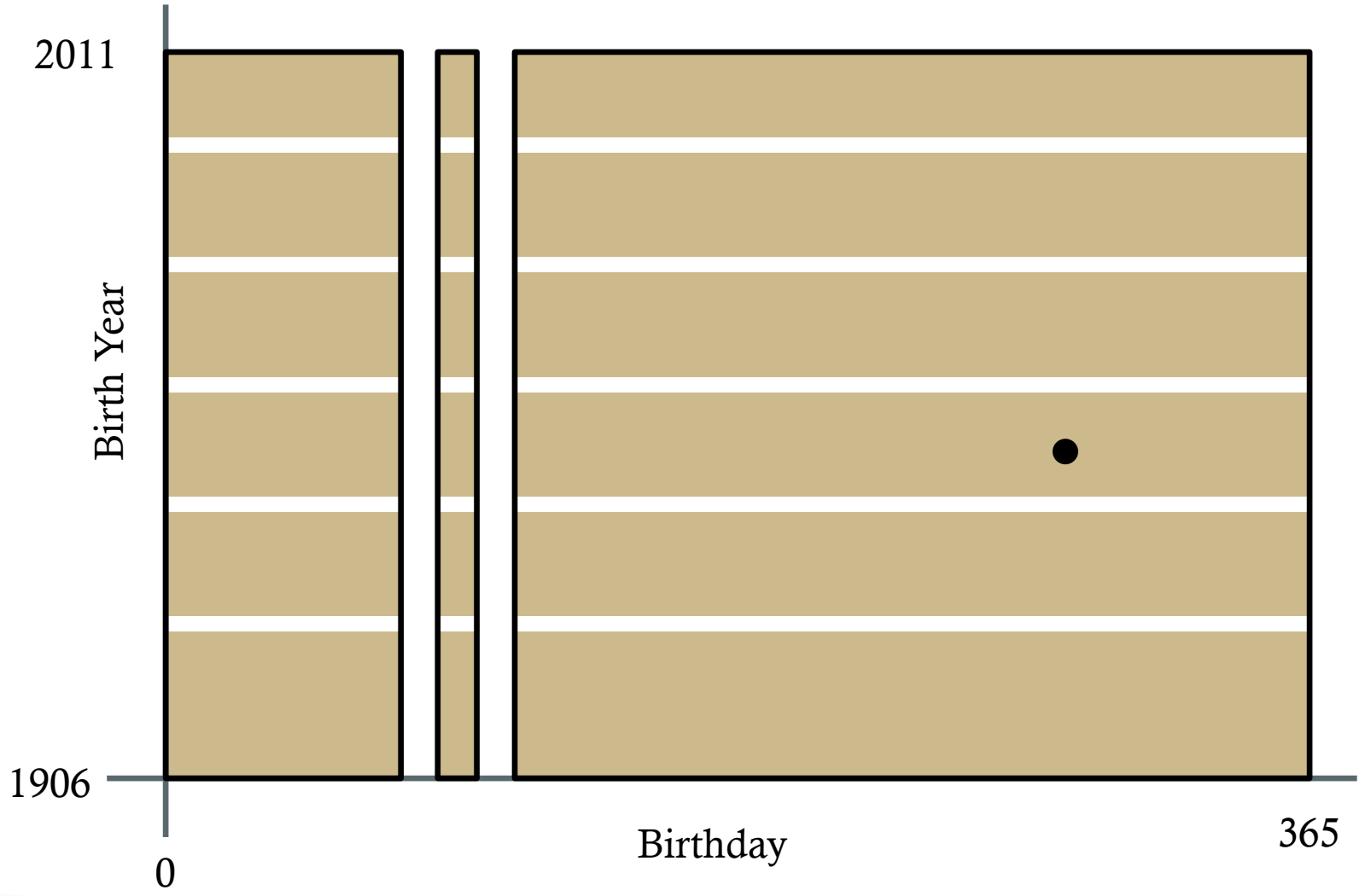
Allow *approximation.*

But only **sound** approximation…

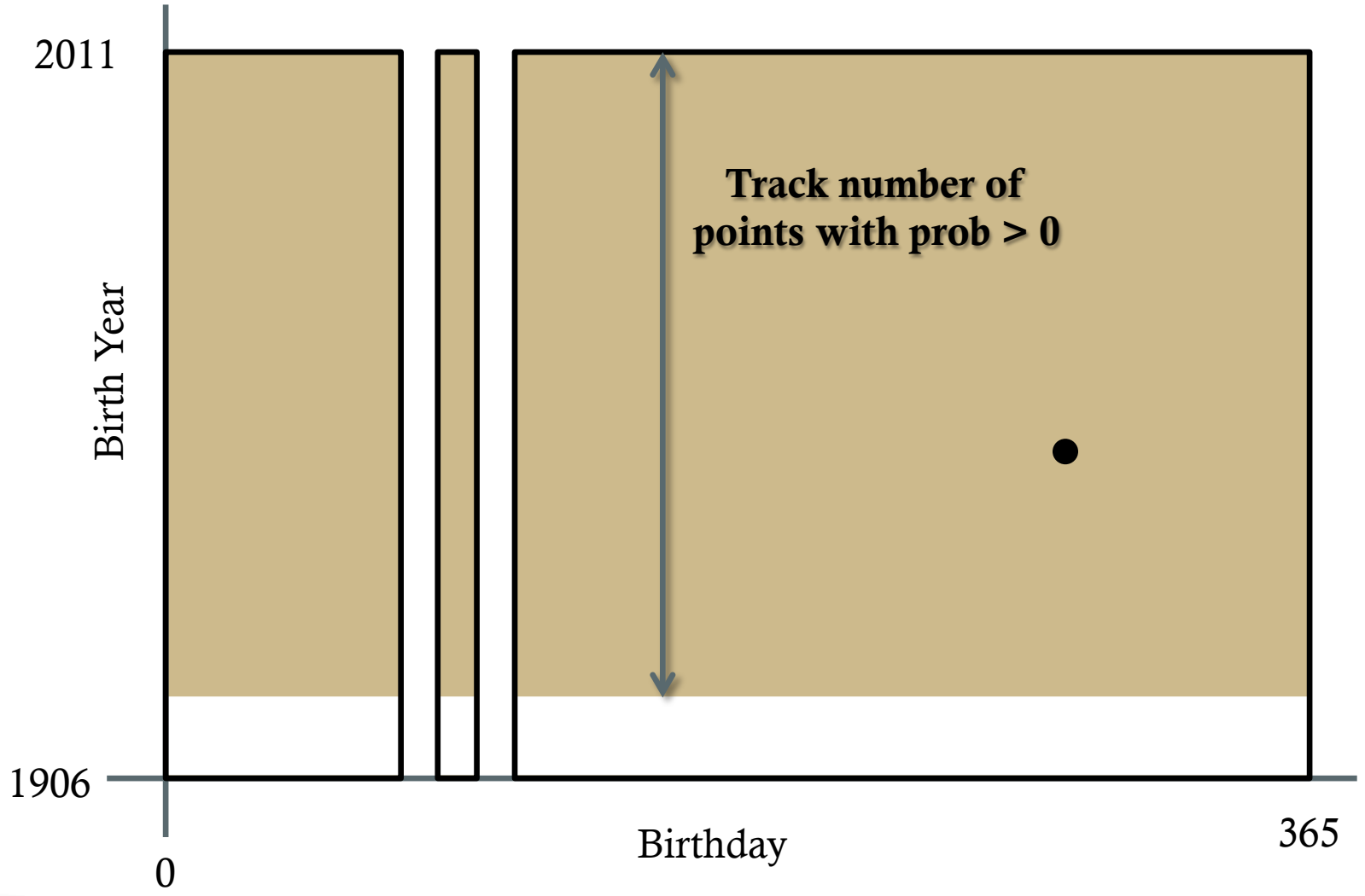
Abstraction



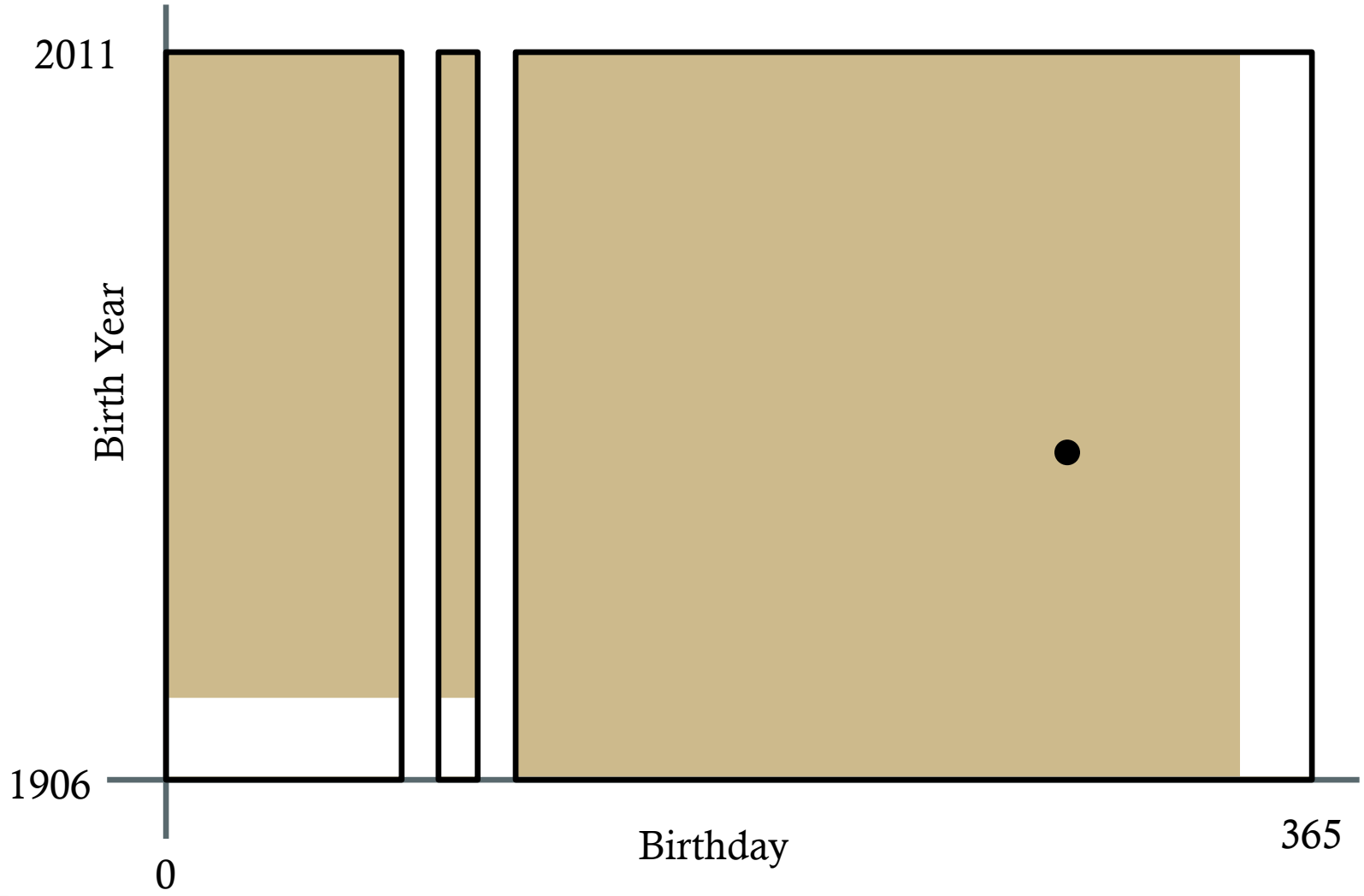
Abstraction



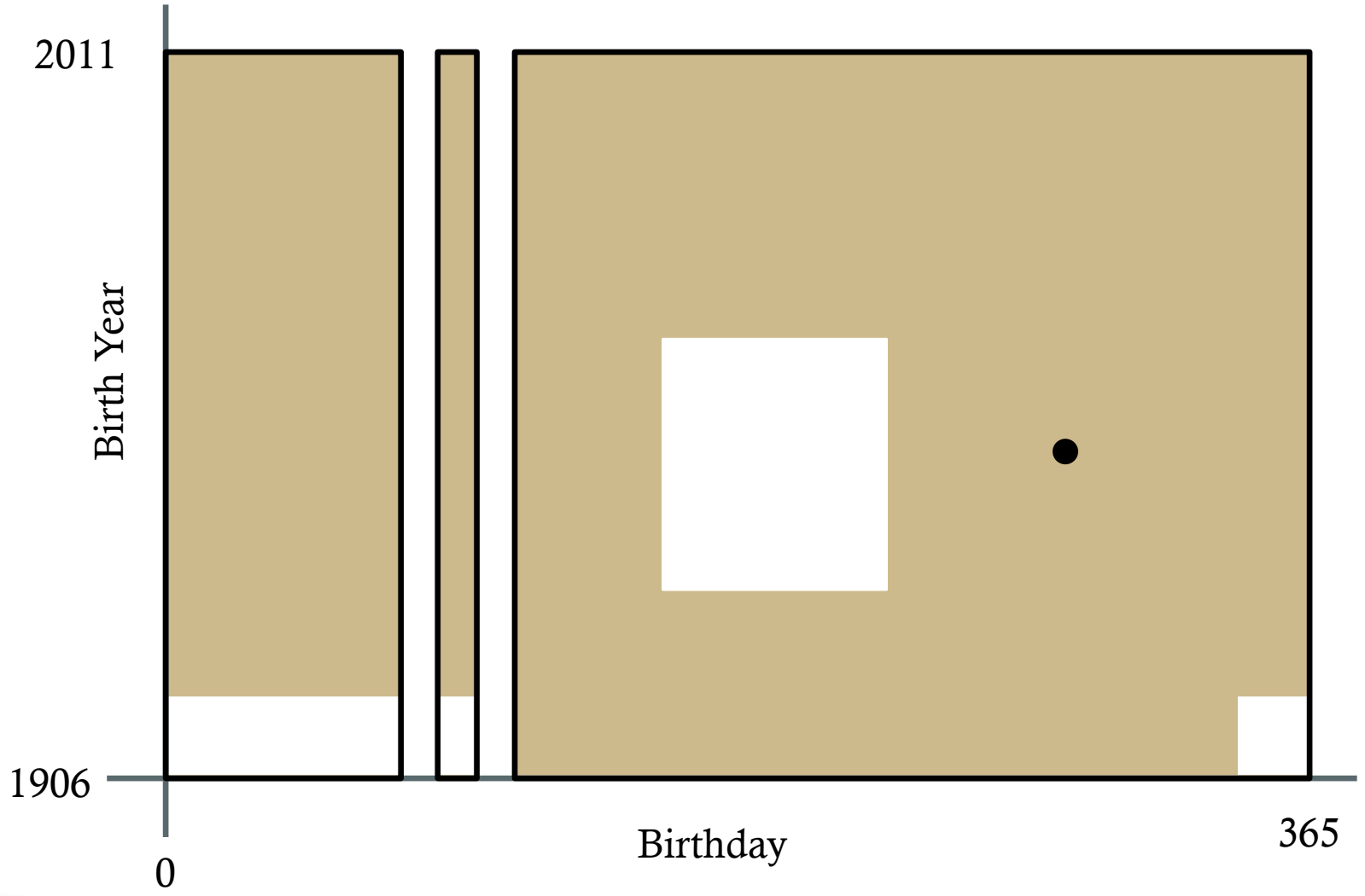
Abstraction



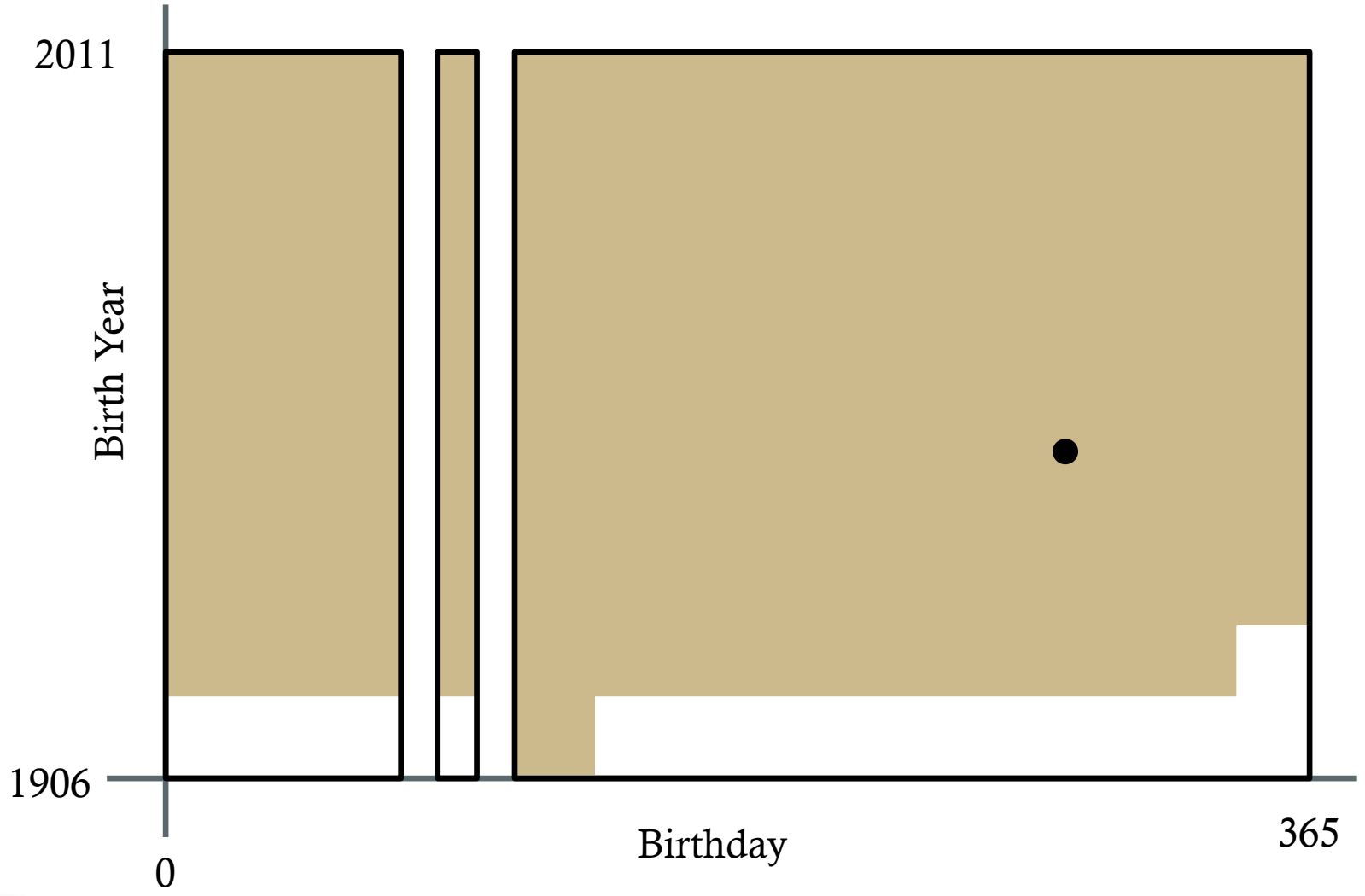
Abstraction



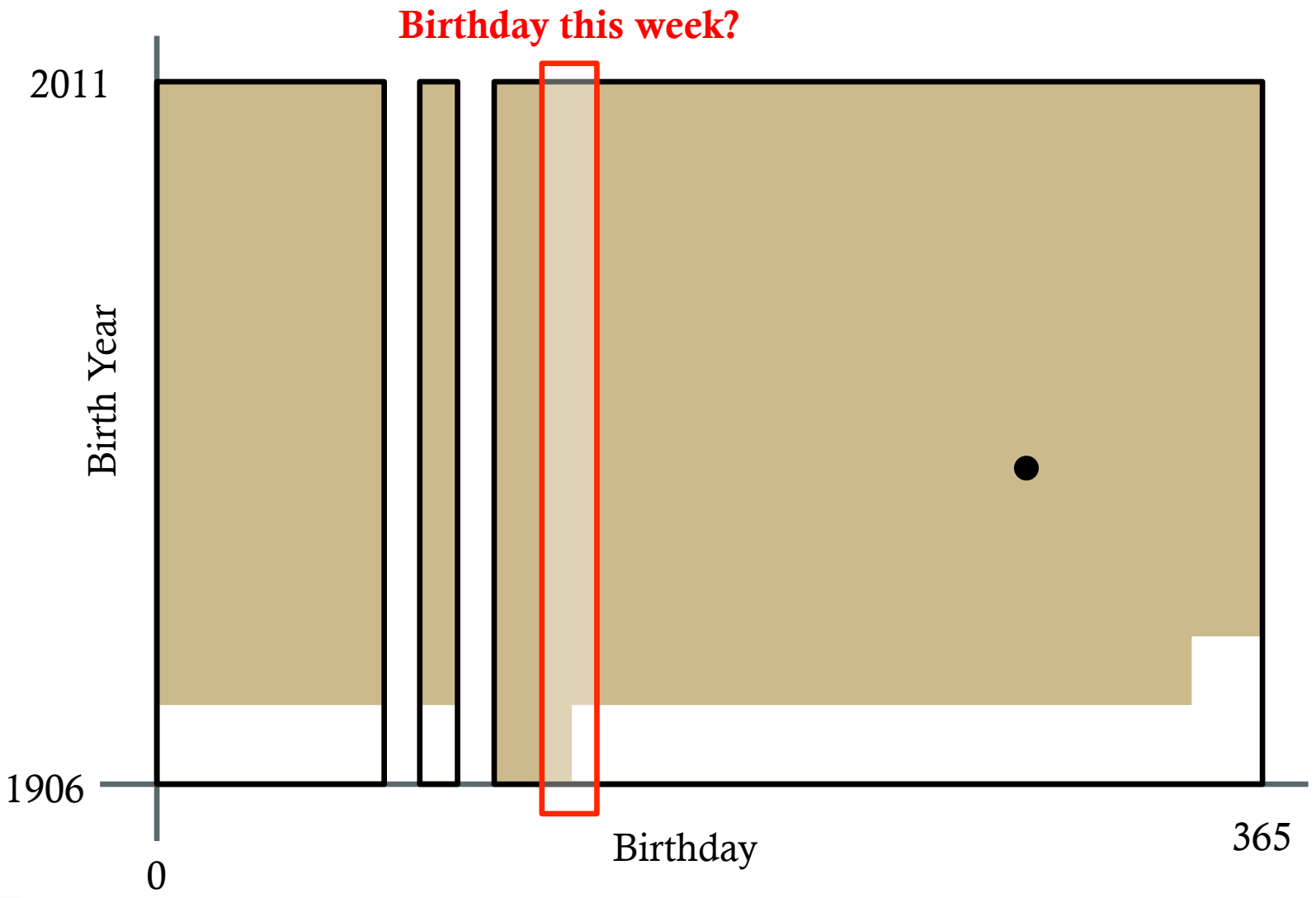
Abstraction



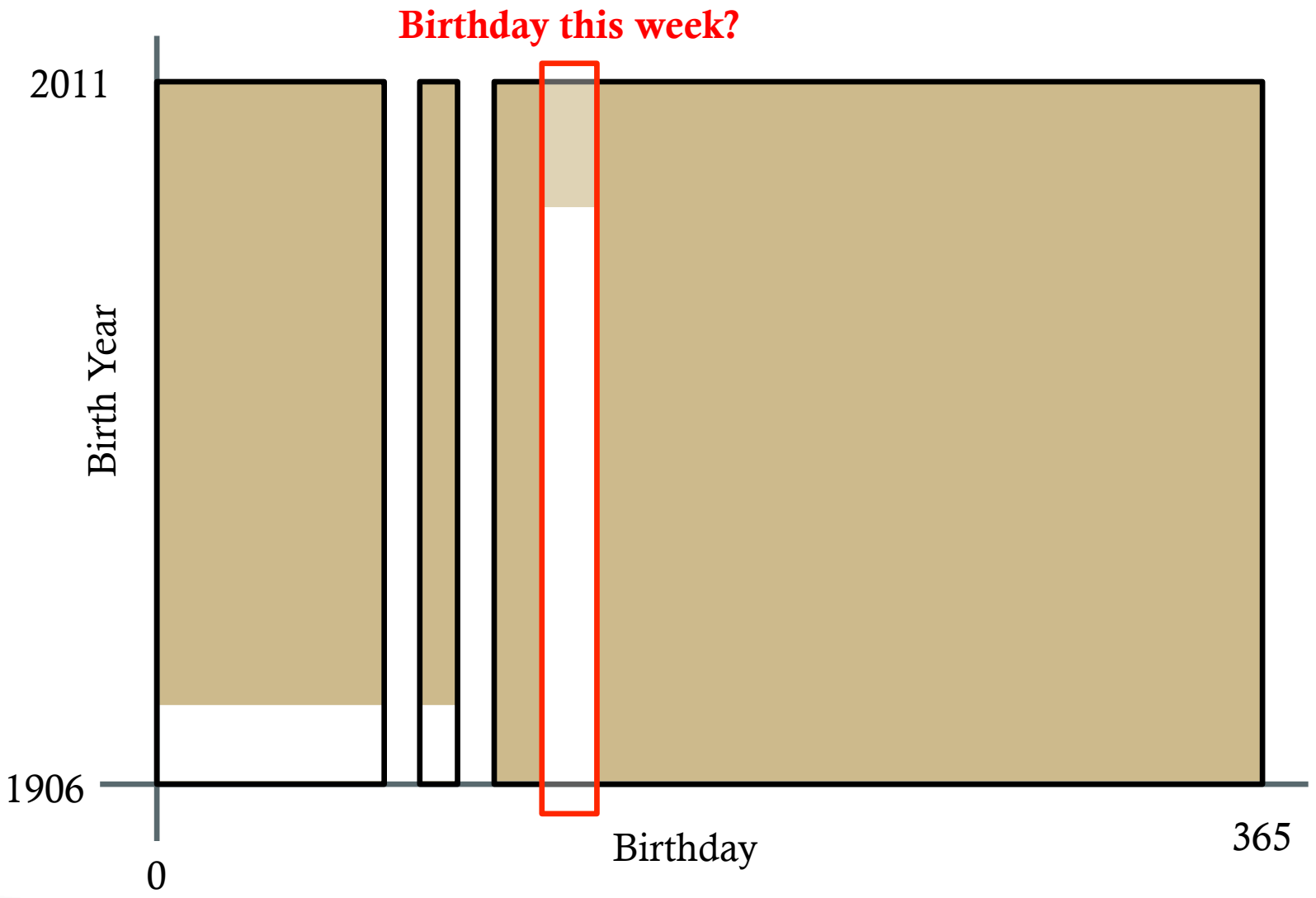
Abstraction



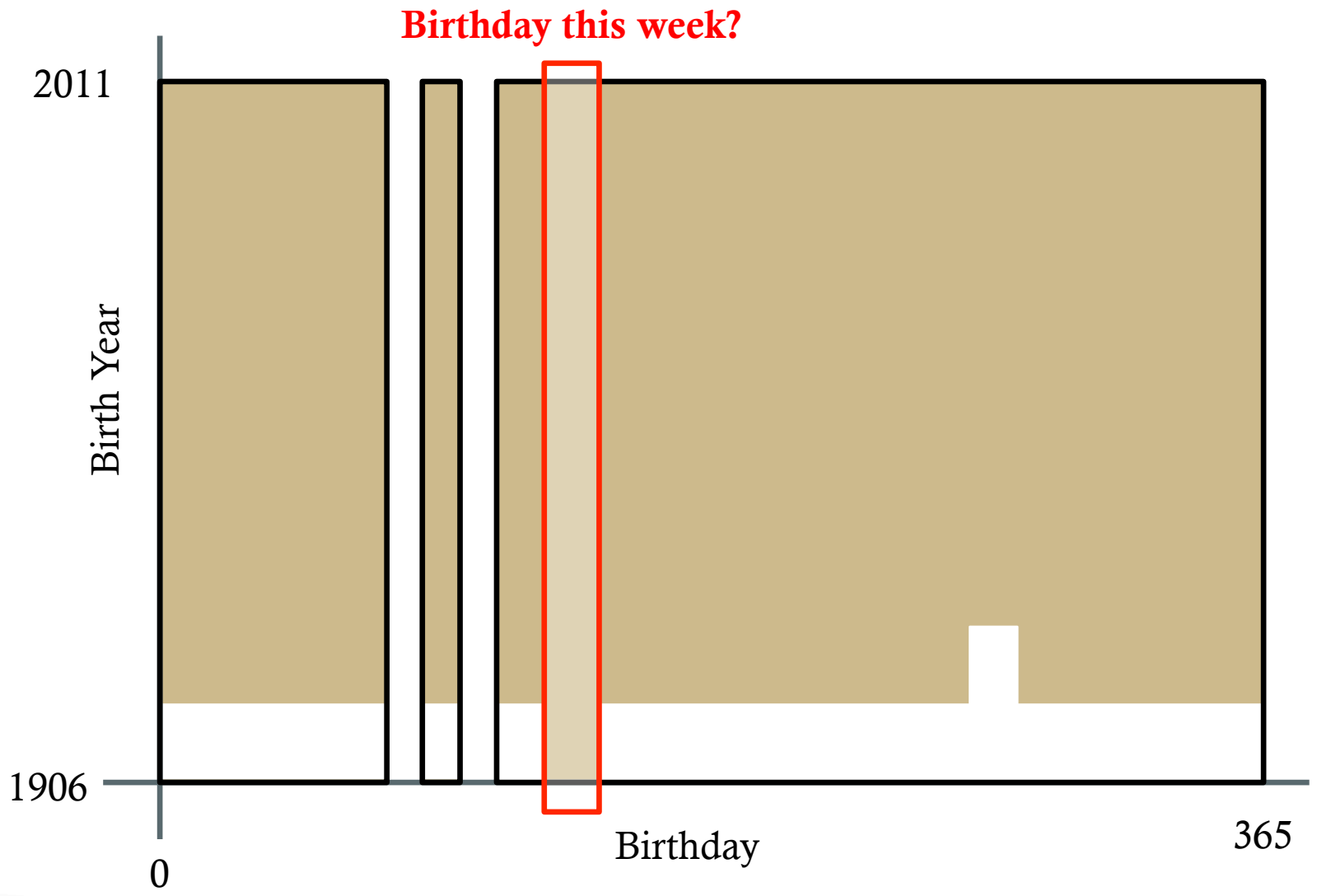
Abstraction



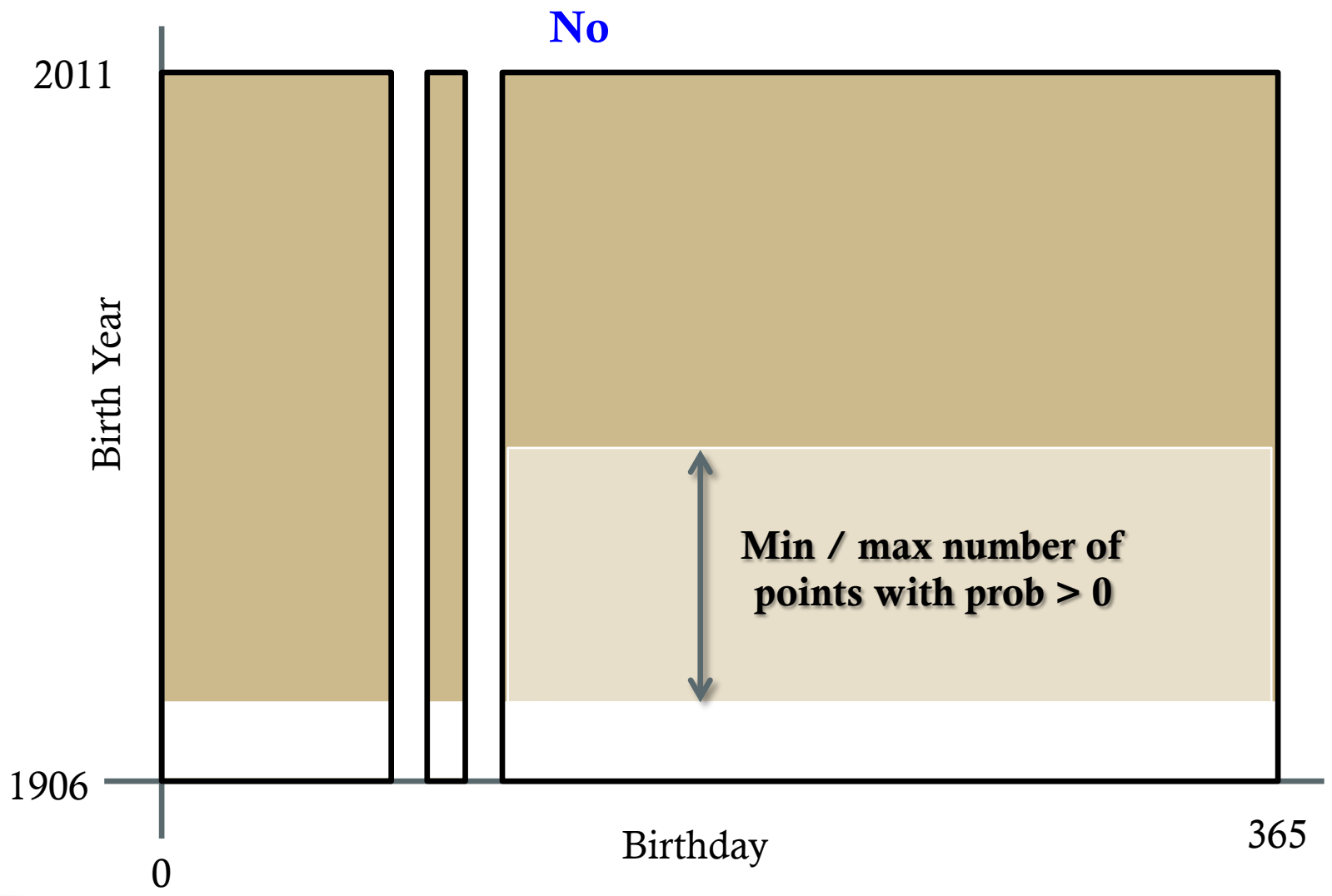
Abstraction



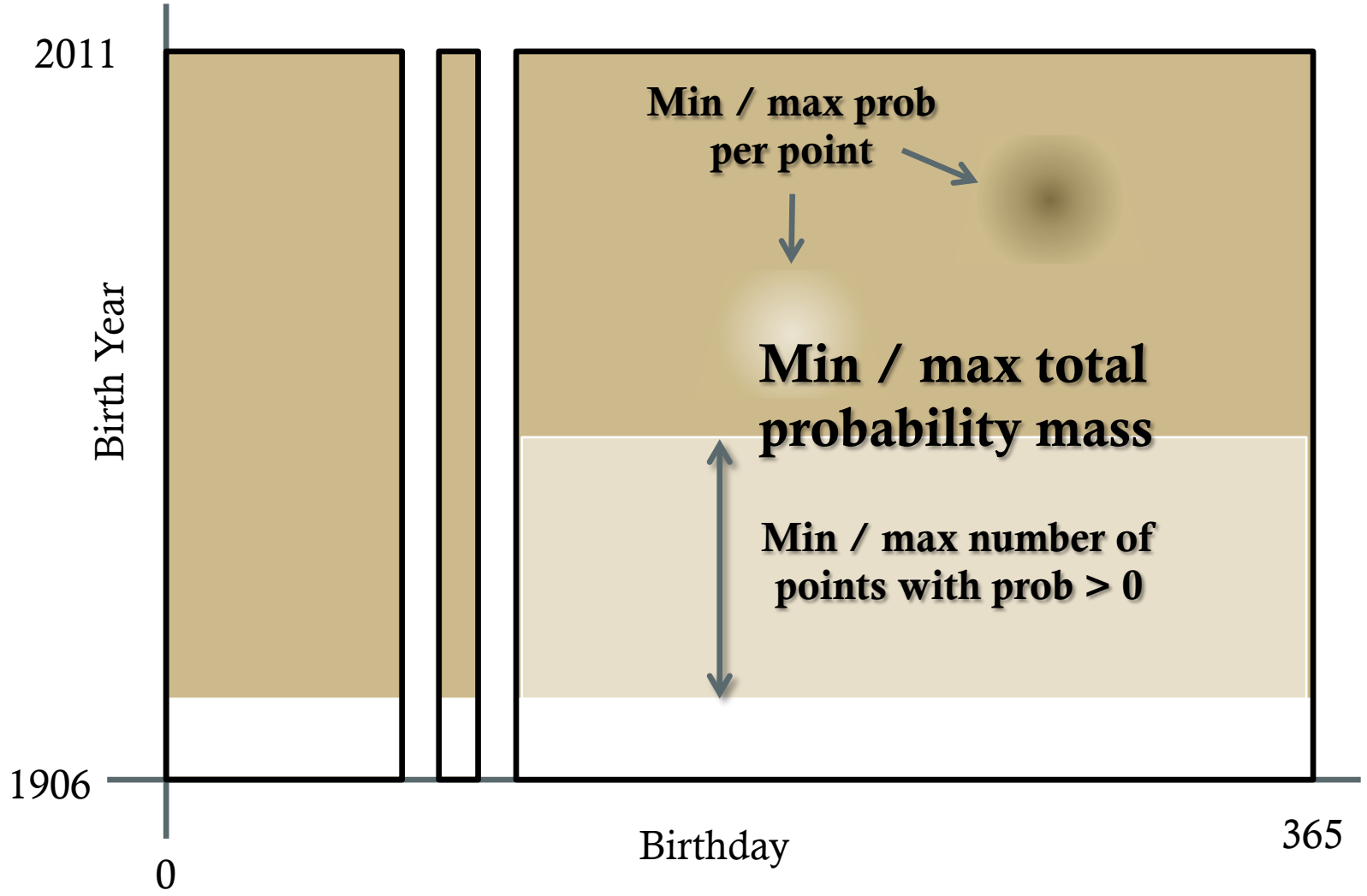
Abstraction



Abstraction



Abstraction



Soundness Theorem

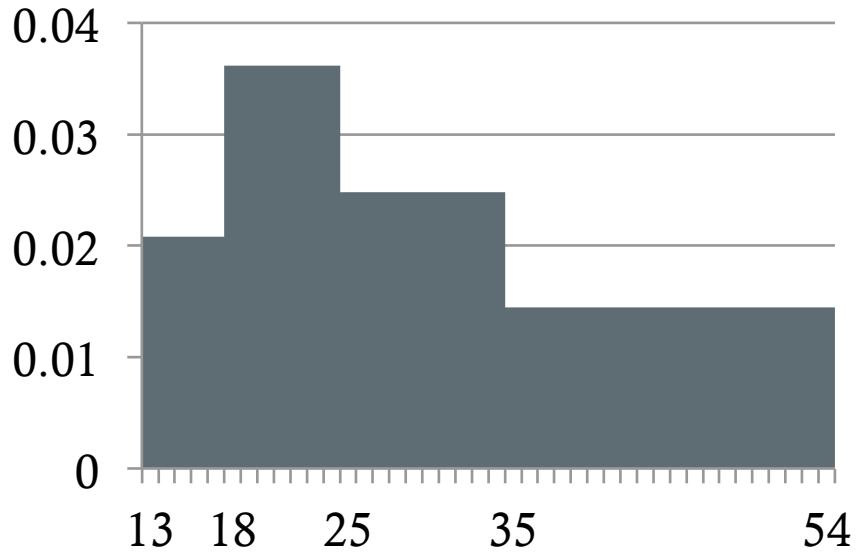
If evaluation using our approach indicates the query does not reveal too much…

Then the query is safe.

No amount of computation on an attacker's part can provide certainty above the threshold.

Caveat

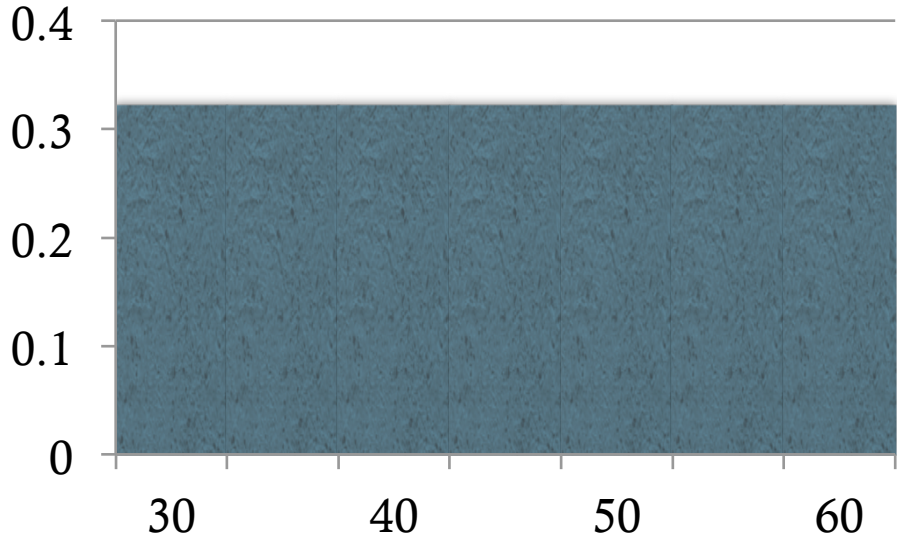
Assuming the initial belief was accurate.



Caveat

Assuming the initial belief was accurate.

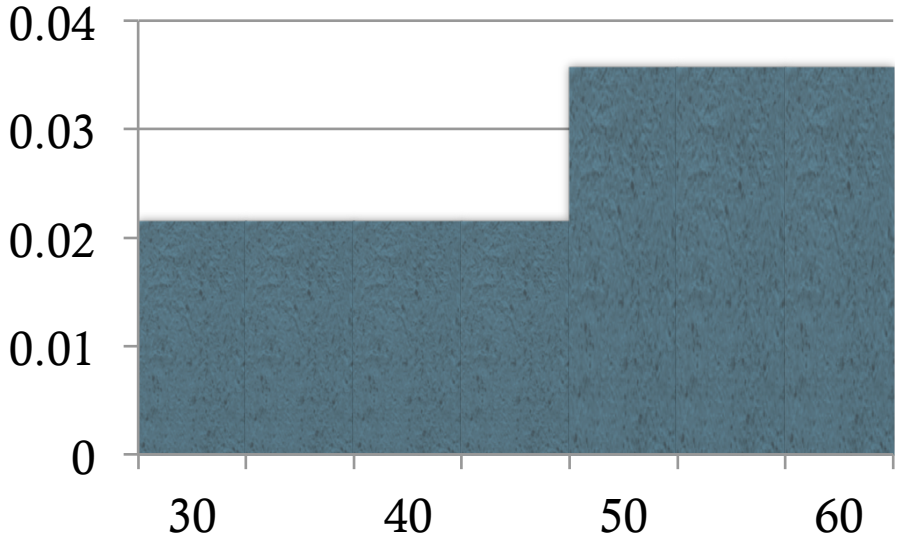
"Ages span 30 – 60 and no age is more than twice as likely as another."



Caveat

Assuming the initial belief was accurate.

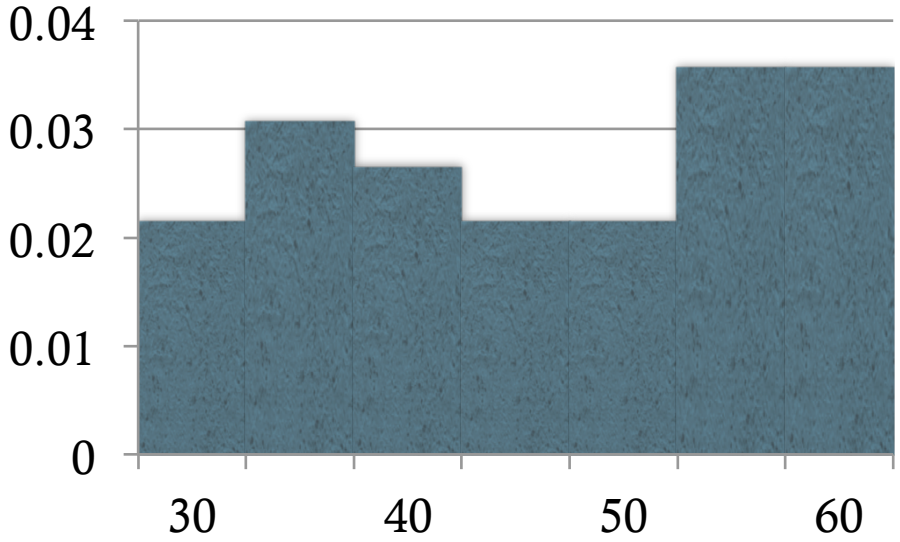
"Ages span 30 – 60 and no age is more than twice as likely as another."



Caveat

Assuming the initial belief was accurate.

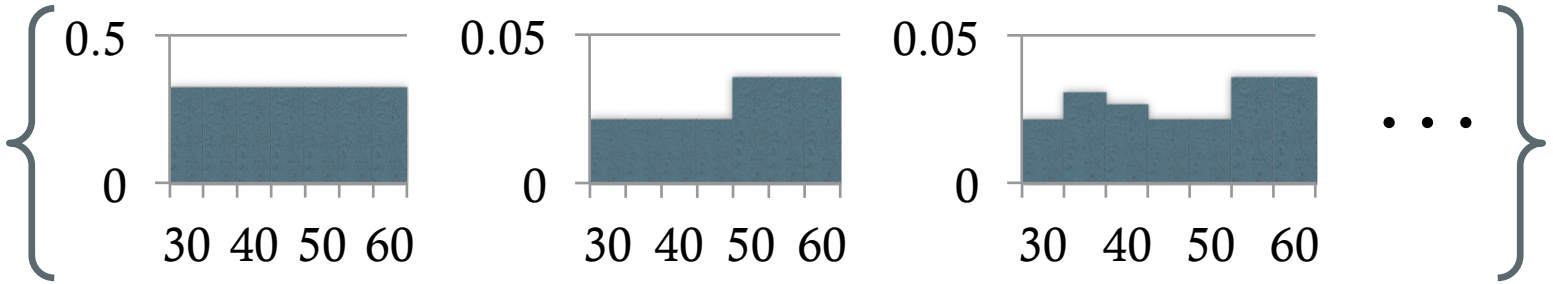
"Ages span 30 – 60 and no age is more than twice as likely as another."



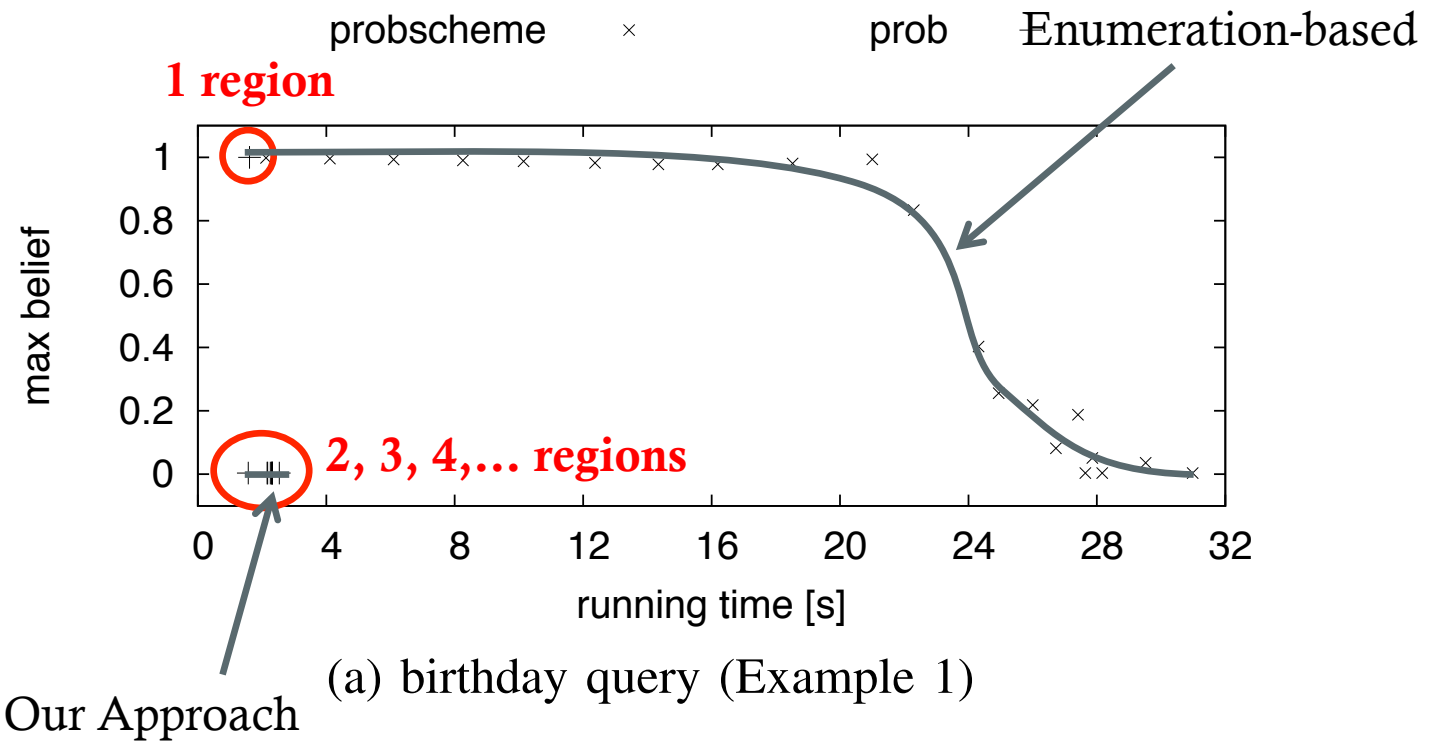
Caveat

Assuming the initial belief was accurate.

"Ages span 30 – 60 and no age is more than twice as likely as another."

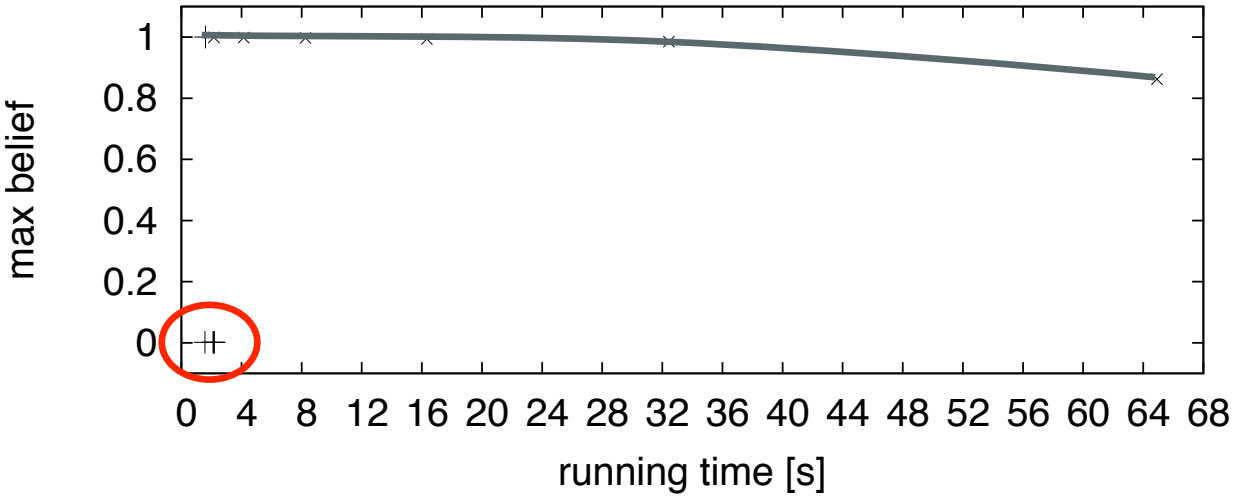


Experiments



(a) birthday query (Example 1)

Experiments



(b) birthday query (Example 1), larger state space

Summary

- Control Information Flow By Focusing on Queries
- No need to introduce noise (querier gets precise results)
- Sound, efficient abstraction for probability distributions
  - Tracks bounds on outsiders' beliefs
- Future work
  - Non-linear assignments
  - Non-integer values (in particular: lists)