Jean Goubault-Larrecq

Randomized complexity classes

Today: **BPP** (part 1)

Today

- Two-sided error: **BPP**
- Error reduction, voting, Chernoff's bound
- The Sipser-Gács-Lautemann theorem

Our third probabilistic class: **BPP**

(also sometimes known as the class of *Metropolis* languages, although some speak of Monte Carlo here again)

http://fr.casino-jackpot.com/wp-content/uploads/2018/04/casino-monaco.jpg
https://upload.wikimedia.org/wikipedia/commons/5/56/Nicholas_Metropolis_cropped.PNG

BPP: Bounded Prob. of Error Polynomial time

- A language L is in **BPP** if and only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):
- if $x \in L$ then $\Pr_r [\mathcal{M}(x,r) \text{ accepts}] \geq 2/3$
- if $x \notin L$ then $\Pr_r [\mathcal{M}(x,r) \text{ accepts}] \leq 1/3$.

i.e. there is also a **polynomial $p(n)$** / $\mathcal{M}(x,r)$ terminates in time $\leq p(n)$, where $n=|x|$, in the worst case (and for any value of r)

… hence, implicitly, we require $|r| \geq p(n)$ (let us say $|r| = p(n)$)

probability taken over all $r \in \{0,1\}^{p(n)}$

two-sided error: $\Pr_r [\mathcal{M}(x,r) \text{ errs}] \leq 1/3$

Examples

https://compeap.com/wp-content/uploads/Land-of-I-Dont-Know.jpg

page | discussion | view source | history

PolyMath

The complexity class BPP

Examples

The problem of determining whether a multivariate polynomial vanishes is in BPP. The idea of the randomized algorithm is to compute the polynomial at a small number of randomly chosen points. For a non-zero polynomial the probability that it vanishes at all those points decreases rapidly with the number of points, and so if it vanishes at all those points we can say with some confidence that the polynomial vanishes everywhere. This problem is also in co-RP, since if the polynomial really does vanish everywhere, then the algorithm is guaranteed to output 1.

It would be good to have more examples. In particular, it would be nice to have an example that isn't obviously in RP or co-RP.

https://asone.ai/polymath/index.php?title=The_complexity_class_BPP

Error reduction

- What is so special about error 1/3?
- Nothing!
- **Theorem.** $\forall\ \varepsilon \in\ ]0, 1/2[$, **BPP** = **BPP**($\varepsilon$).
- Note: **BPP**=**BPP**(1/3) (def.)
  BPP(ε)={*all languages*} if $\varepsilon \geq 1/2$…
  BPP(0)=**P**

error = 1/3 here

A language L is in **BPP** if and only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

if $x \in L$ then $\Pr_r\,[\mathcal{M}(x,r) \text{ accepts}] \geq 2/3$

if $x \notin L$ then $\Pr_r\,[\mathcal{M}(x,r) \text{ accepts}] \leq 1/3$.

A language L is in **BPP**(ε) and only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

if $x \in L$ then $\Pr_r\,[\mathcal{M}(x,r) \text{ accepts}] \geq 1-\varepsilon$

if $x \notin L$ then $\Pr_r\,[\mathcal{M}(x,r) \text{ accepts}] \leq \varepsilon$

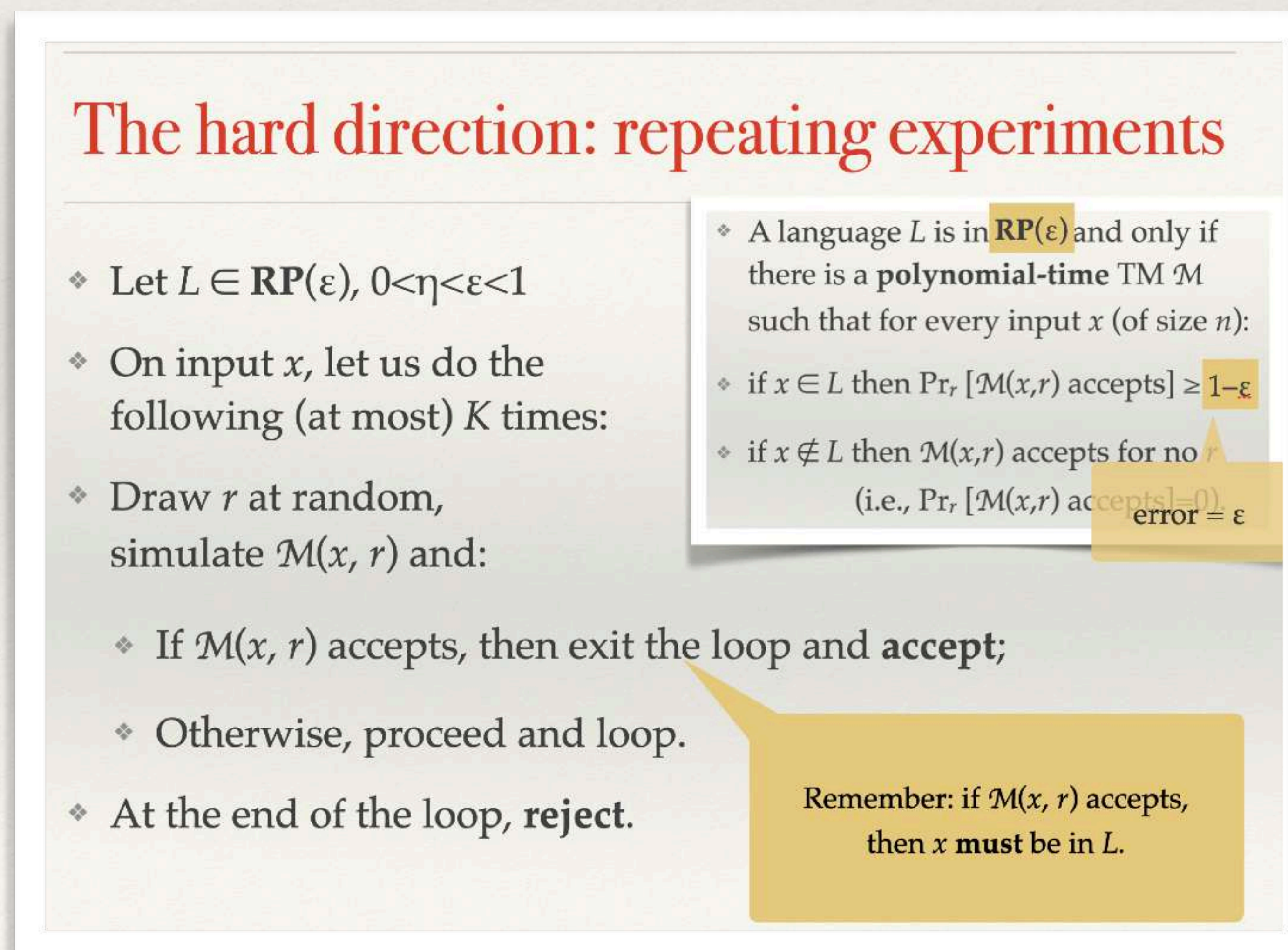
error = ε

The easy cases: error amplification(!)

- Clearly, if $\eta \leq \varepsilon$ then
  BPP(η) $\subseteq$ **BPP**(ε)
- Note: **BPP**(0)=**P** (sometimes believed $\neq$ **BPP**)
  BPP(ε)={*all languages*} for every $\varepsilon \geq 1/2$
- In the middle, hence, we will see that all the intermediate **BPP**(ε) ($\varepsilon \in]0, 1/2[$) are equal to **BPP**.

Error reduction

- We will show that **BPP** (= **BPP**(1/3)) is included in **BPP**(ε) for every ε ∈]0, 1/2[, arbitrarily close to 0.
- The technique we used for **RP** does **not** work: why?
- Hence we must proceed differently



Majority voting

- Imagine running $\mathcal{M}(x,r)$ for various values of r, and **tallying the votes**
- Redo the vote N times (here N=4)
- Here 3 accepts / 1 reject ⇒ majority is for **acceptance**

Majority voting

- This is typical of what happens when $x \in L$: running a large number of votes should produce a majority of **accepts**, with **high probability**
- … but how high?

<u>Outcome</u>

accept

accept

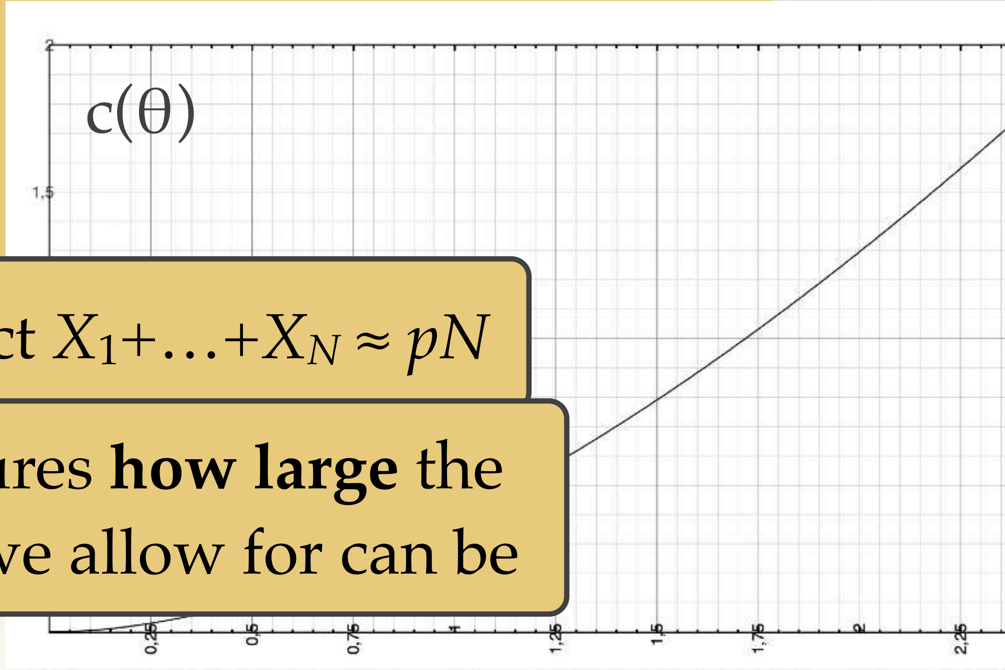
reject

accept

Chernoff's bound

- Intuitive contents:
  Imagine Pr(**yes**) = p
  Then Pr(proportion of **yes**es among N voters is close to p)
  goes to 1 **exponentially fast** as $N \to \infty$.

- **Theorem.** Let $X_1, \ldots, X_N$ be **independent** rand. vars
  with values in $\{0, 1\}$ and
  with the **same law**: $\Pr(X_i=1)=p$.
  Then $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
  $\leq \exp(-c(\theta)pN)$



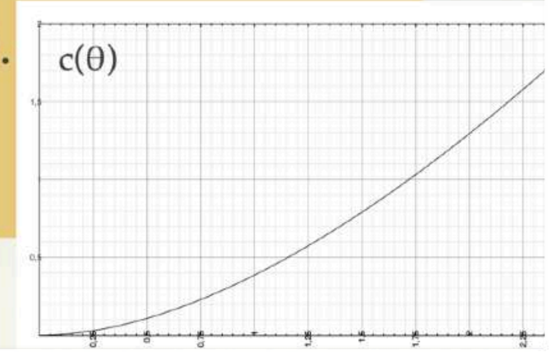
We expect $X_1+\ldots+X_N \approx pN$

$1+\theta$ measures **how large** the deviation we allow for can be

For all practical purposes, $c(\theta) \approx \theta^2/3$

Proof of Chernoff's bound (1/4)

Theorem. Let $X_1, \ldots, X_N$ be **independent** rand. vars
with values in $\{0, 1\}$ and
with the **same law**: $\Pr(X_i=1)=p$.
Then $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
$\leq \exp(-c(\theta)pN)$



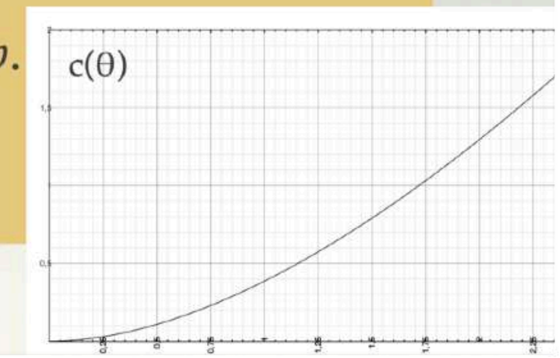
- Let $t, a > 0$ to be fixed later
- Define the rand. var $X = \exp(t(X_1+\ldots+X_N))$
- Note that $E(X) \leq \exp(tN) < \infty$, so we can use **Markov's inequality**:

$$\Pr(X \geq a.E(X)) \leq 1/a$$

Theorem (Markov's inequality).
Let X be a **non-negative real-valued** random variable
with **finite** expectation $E(X)$. For every $a \geq 0$:
$\Pr(X \geq a.E(X)) \leq 1/a$.

Proof of Chernoff's bound (2/4)

Theorem. Let $X_1, \ldots, X_N$ be **independent** rand. vars with values in $\{0, 1\}$ and with the **same law**: $\Pr(X_i=1)=p$.
Then $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN) \leq \exp(-c(\theta)pN)$

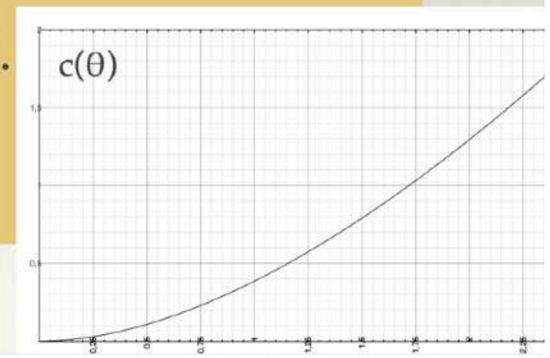


- Let $t, a > 0$ to be fixed later
- Define the rand. var $X = \exp(t(X_1+\ldots+X_N))$
- $\Pr(X \geq a.E(X)) \leq 1/a$ (from last slide)
- Let us fix $a = \exp(t(1+\theta)pN) / E(X)$, hence:
- $\Pr(X \geq \exp(t(1+\theta)pN)) \leq E(X) \exp(-t(1+\theta)pN))$

This is just $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$

Proof of Chernoff's bound (3/4)

Theorem. Let $X_1, \ldots, X_N$ be **independent** rand. vars
with values in $\{0, 1\}$ and
with the **same law**: $Pr(X_i=1)=p$.
Then $Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
$\leq \exp(-c(\theta)pN)$



- Let $t>0$, to be fixed later
- $X = \exp(t(X_1+\ldots+X_N))$
- $Pr(X_1+\ldots+X_N \geq (1+\theta)pN) \leq E(X) \exp(-t(1+\theta)pN))$ (from last slide)
- $E(X) = E(\Pi_{i=1}^N \exp(tX_i))$

  $= \Pi_{i=1}^N E(\exp(tX_i))$ (**independence**)

  $= \Pi_{i=1}^N (p \exp(t) + 1-p)$ (def. of the **law** of X_i)

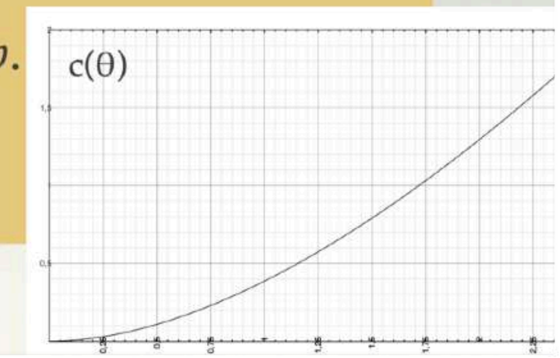
  $= (p \exp(t) + 1-p)^N$

  $= (1+p(\exp(t)-1))^N \leq \exp((\exp(t)-1)pN)$

take logs:
$N \log(1+p(\exp(t)-1)) \leq Np(\exp(t)-1)$

Proof of Chernoff's bound (4/4)

Theorem. Let $X_1, \ldots, X_N$ be **independent** rand. vars
with values in {0, 1} and
with the **same law**: $\Pr(X_i=1)=p$.
Then $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
$\leq \exp(-c(\theta)pN)$



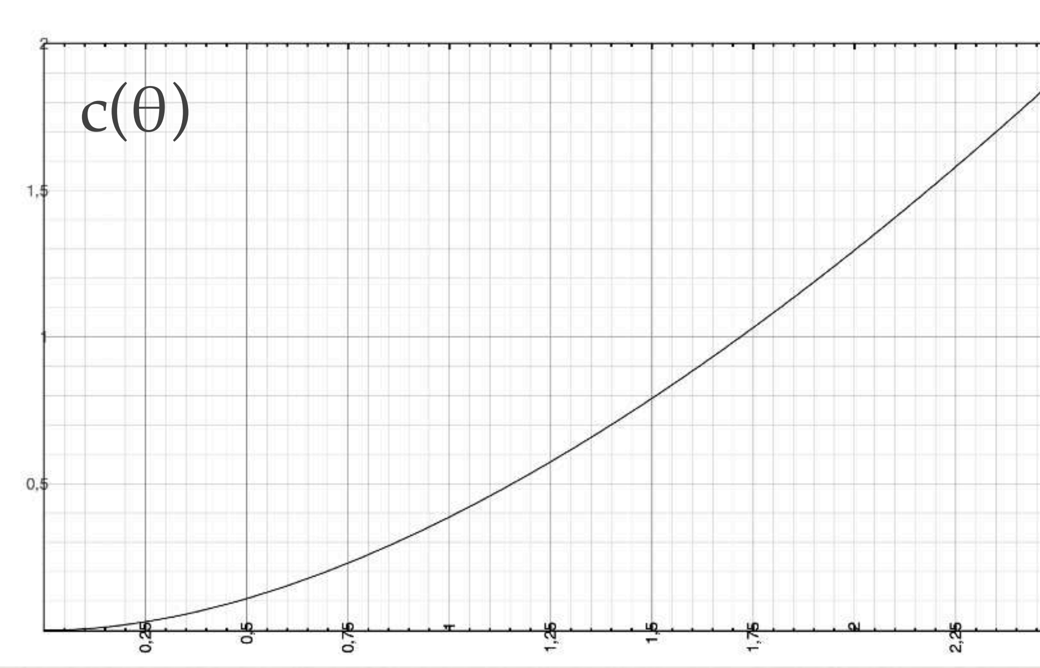
- Let $t>0$, to be fixed later
- $X = \exp(t(X_1+\ldots+X_N))$
- $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
  $\leq \exp((\exp(t)-1)pN) \exp(-t(1+\theta)pN))$
  (from last slide)
- Let $t = \log(1+\theta)$, so $(\exp(t)-1)pN = \theta pN$, hence
- $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
  $\leq \exp((\theta-(1+\theta)\log(1+\theta))pN)$.

Call this $-c(\theta)$

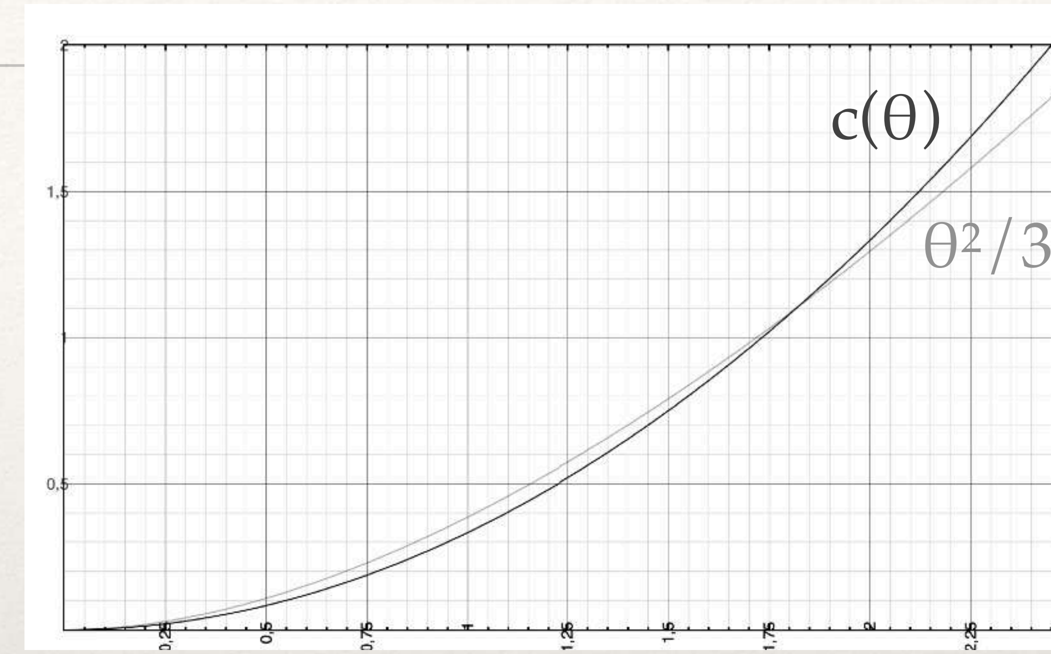
Done! □

A few properties of $c(\theta) = -\theta + (1+\theta)\log(1+\theta)$

- **Prop 1.** $c(\theta)$ is monotonic (for $\theta \geq 0$)
- *Proof.* $c'(\theta) = \log(1+\theta) \geq 0$



A few properties of $c(\theta)=-\theta+(1+\theta)\log(1+\theta)$



- **Prop 1.** $c(\theta)$ is monotonic (for $\theta \geq 0$)
- **Prop 2.** For $0 \leq \theta \leq 1$, $c(\theta) \geq \theta^2/3$
- *Proof.* $c(0)=0$

  $c'(0)=0$ (recall $c'(\theta) = \log(1+\theta)$)

  $c''(0)=1$ ($c''(\theta) = 1/(1+\theta)$)

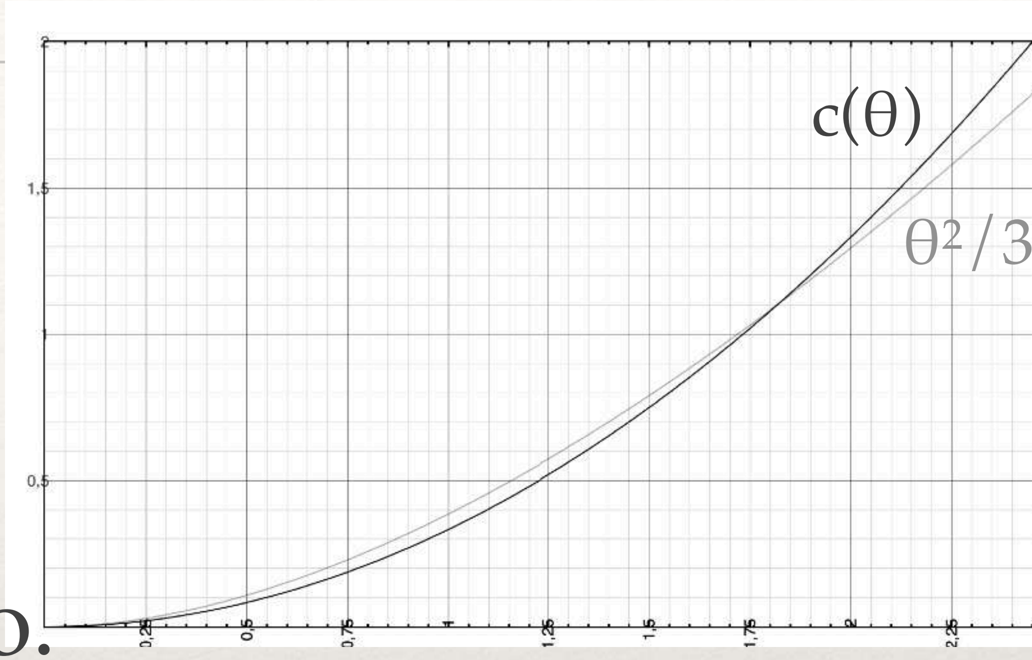
  $c'''(0)=-1$ ($c'''(\theta) = -1/(1+\theta)^2$)

- So $c(\theta) = \theta^2/2 - \theta^3/6 + c^{(4)}(\theta_0)/24$ for some $0 \leq \theta_0 \leq \theta$ (Taylor)

  $\geq \theta^2/2 - \theta^3/6$ (since $c^{(4)}(\theta) = 2/(1+\theta)^3 \geq 0$)

  $\geq \theta^2/3$ (since $\theta \leq 1$) □

A few properties of $c(\theta)=-\theta+(1+\theta)\log(1+\theta)$



- **Prop 1.** $c(\theta)$ is monotonic (for $\theta \geq 0$)
- **Prop 2.** For $0 \leq \theta \leq 1$, $c(\theta) \geq \theta^2/3$
- **Prop 3.** $c(\theta)/(1+\theta)$ is monotonic too.
- Proof. $c(\theta)/(1+\theta) = -\theta/(1+\theta) + \log(1+\theta)$

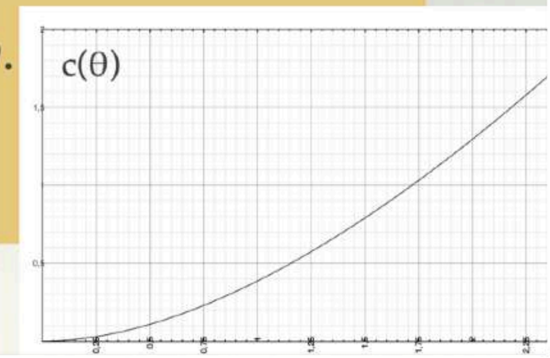
  Derivative: $-1/(1+\theta)^2 + 1/(1+\theta) = \theta/(1+\theta)^2 \geq 0$ □

Application to voting (1/4)

- Assume that $\Pr_r(\mathcal{M}(x,r)$ errs$) \leq 1/3$,
  what is the probability P that more than 1/2 of N votes
  $\mathcal{M}(x,r_1), \ldots, \mathcal{M}(x,r_N)$ err?

Theorem. Let $X_1, \ldots, X_N$ be **independent** rand. vars
with values in {0, 1} and
with the **same law**: $\Pr(X_i=1)=p$.
Then $\Pr(X_1+\ldots+X_N \geq (1+\theta)pN)$
$\leq \exp(-c(\theta)pN)$

(Chernoff)



- Let $X_i = 1$ iff $\mathcal{M}(x,r_i)$ errs:
  all assumptions satisfied
  with $p \leq 1/3$

- Take $\theta = 1/(2p) - 1$, so $(1+\theta)p = 1/2$: $\quad P \leq \exp(-c(\theta)pN)$

Application to voting (2/4)

- Assume that $\Pr_r(\mathcal{M}(x,r) \text{ errs}) \leq 1/3$,
  what is the probability P that more than 1/2 of N votes $\mathcal{M}(x,r_1)$, …, $\mathcal{M}(x,r_N)$ err?
- Take $\theta=1/(2p)-1$, so $(1+\theta)p = 1/2$: $\quad$ $P \leq \exp(-c(\theta)pN)$
  (from last slide)

Prop 1. $c(\theta)$ is monotonic (for $\theta \geq 0$)

Prop 2. For $0 \leq \theta \leq 1$, $c(\theta) \geq \theta^2/3$

Prop 3. $c(\theta)/(1+\theta)$ is monotonic too.

- I.e., $P \leq \exp(-c(\theta)/(1+\theta) \,.\, 1/2\, N)$
- $\leq \exp(-c(1/2)/(3/2) \,.\, 1/2\, N)$
  (since $p \leq 1/3$, so $\theta \geq 1/2$; plus Prop 3)
- $\leq \exp(-(1/2)^2/3/(3/2) \,.\, 1/2\, N)$ $\quad$ (Prop 2)
  $= \exp(-N/36)$

Application to voting (3/4)

- Assume that $\Pr_r(\mathcal{M}(x,r) \text{ errs}) \leq 1/3$, what is the probability P that more than 1/2 of N votes $\mathcal{M}(x,r_1), \ldots, \mathcal{M}(x,r_N)$ err?
- Answer: at most $\exp(-N/36)$

Error reduction for **BPP**

- First, a useful trick.
  Let us say that $\mathcal{M}(x,r)$ **errs**
  iff ($x \in L$ and $\mathcal{M}(x,r)$ rejects)
  or ($x \notin L$ and $\mathcal{M}(x,r)$ accepts)
- (That used to be implicit.)
- Then:

A language L is in **BPP** if and only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

$$\Pr_r [\mathcal{M}(x,r) \text{ errs}] \leq 1/3.$$

A language L is in **BPP**(ε) nd only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

$$\Pr_r [\mathcal{M}(x,r) \text{ errs}] \leq \varepsilon.$$

error = ε

Error reduction for **BPP**

- Let L be in **BPP**, as here →
- Build new rand. TM $\mathcal{M}'$ by:
- `yeas` := 0
  `for` i=1 to N:
  draw r at random
  if $\mathcal{M}(x,r)$ accepts:
  `yeas++`
  accept if `yeas`$\geq N/2$, else **reject**

A language L is in **BPP** if and only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

$$\Pr_r\,(\mathcal{M}(x,r) \text{ errs}) \leq 1/3.$$

A language L is in **BPP(ε)** nd only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

$$\Pr_r\,(\mathcal{M}(x,r) \text{ errs}) \leq \varepsilon.$$

error = ε

Error reduction for **BPP**

- Let L be in **BPP**
- Build new rand. TM $\mathcal{M}$' by:
- `yeas` := 0
  `for` i=1 to N:
  draw r at random
  if $\mathcal{M}(x,r)$ accepts:
  `yeas`++
  accept if `yeas`$\geq N/2$, else **reject**

- $\mathcal{M}$' errs on input x iff at least half of the calls to $\mathcal{M}(x,r)$ err
- That happens with probability $\leq \exp(-N/36)$
- … $\leq \varepsilon$ provided that we pick $N \geq -36 \log \varepsilon$

Note: if $\mathcal{M}$ runs in polytime $p(n)$,
then $\mathcal{M}$' runs in **polytime** = $-36 \log \varepsilon\ p(n)$ + cst.

Error reduction for **BPP**

- Hence **BPP**(= **BPP**(1/3)) $\subseteq$ **BPP**(ε)
  for ε arbitrarily close to 0
- By a similar argument, we can replace 1/3 by any η, $0<\eta<1/2$, so **BPP**(η) $\subseteq$ **BPP**(ε)
  for ε arbitrarily close to 0
- Recalling that **BPP**(ε) $\subseteq$ **BPP**(η) if $\leq \eta$, we obtain:
- **Theorem.** For every ε, $0< \varepsilon<1/2$, **BPP**=**BPP**(ε).
- … but can we do better?

Application to voting (4/4)

- Assume that $\Pr_r(\mathcal{M}(x,r) \text{ errs}) \leq 1/3$,
  how large should N be so that
  the probability P that more than 1/2
  of N votes $\mathcal{M}(x,r_1), \ldots, \mathcal{M}(x,r_N)$ err
  is $\leq 1/2^{q(n)}$?

- Answer: at least $36\, q(n) \log 2$

- *Proof.* $\exp(-N/36) \leq 1/2^{q(n)}$ iff
  $-N/36 \leq -q(n) \log 2$

The only magical formula
you'll need to remember
for error reduction by majority voting

Note: if $q(n)$ is polynomial,
this is polynomial, too

Application to voting (3/4

- Assume that $\Pr_r(\mathcal{M}(x,r) \text{ errs}) \leq 1/3$,
  what is the probability P that more than 1/2 of N
  $\mathcal{M}(x,r_1), \ldots, \mathcal{M}(x,r_N)$ err?

- Answer: at most $\exp(-N/36)$

Error reduction for **BPP** revisited

- Let L be in **BPP**
- Build new rand. TM $\mathcal{M}'$ by:
- `yeas` := 0
  `for` i=1 to N := 36 $q(n)$ log 2:
  draw r at random
  if $\mathcal{M}(x,r)$ accepts:
  `yeas`++
  accept if `yeas`$\geq N/2$, else **reject**

- $\mathcal{M}'$ errs on input x iff at least half of the calls to $\mathcal{M}(x,r)$ err
- That happens with probability $\leq 1/2^{q(n)}$

Note: if $\mathcal{M}$ runs in polytime $p(n)$, and $q(n)$ is polynomial
then $\mathcal{M}'$ runs in **polytime** = $O(q(n)\, p(n) \log n)$ [log n for operations on the counter i]

Error reduction for **BPP** revisited

A language L is in **BPP**(ε) nd only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

if $x \in L$ then $\Pr_r [\mathcal{M}(x,r) \text{ accepts}] \geq 1-\varepsilon$

if $x \notin L$ then $\Pr_r [\mathcal{M}(x,r) \text{ accepts}] \leq \varepsilon$

error = ε

- **Theorem. BPP** is equal to:
  — **BPP**(ε) for every ε, $0 < \varepsilon < 1/2$
  — **BPP**($1/2^{q(n)}$) for every polynomial $q(n)$

The new landscape

BPP vs. other complexity classes

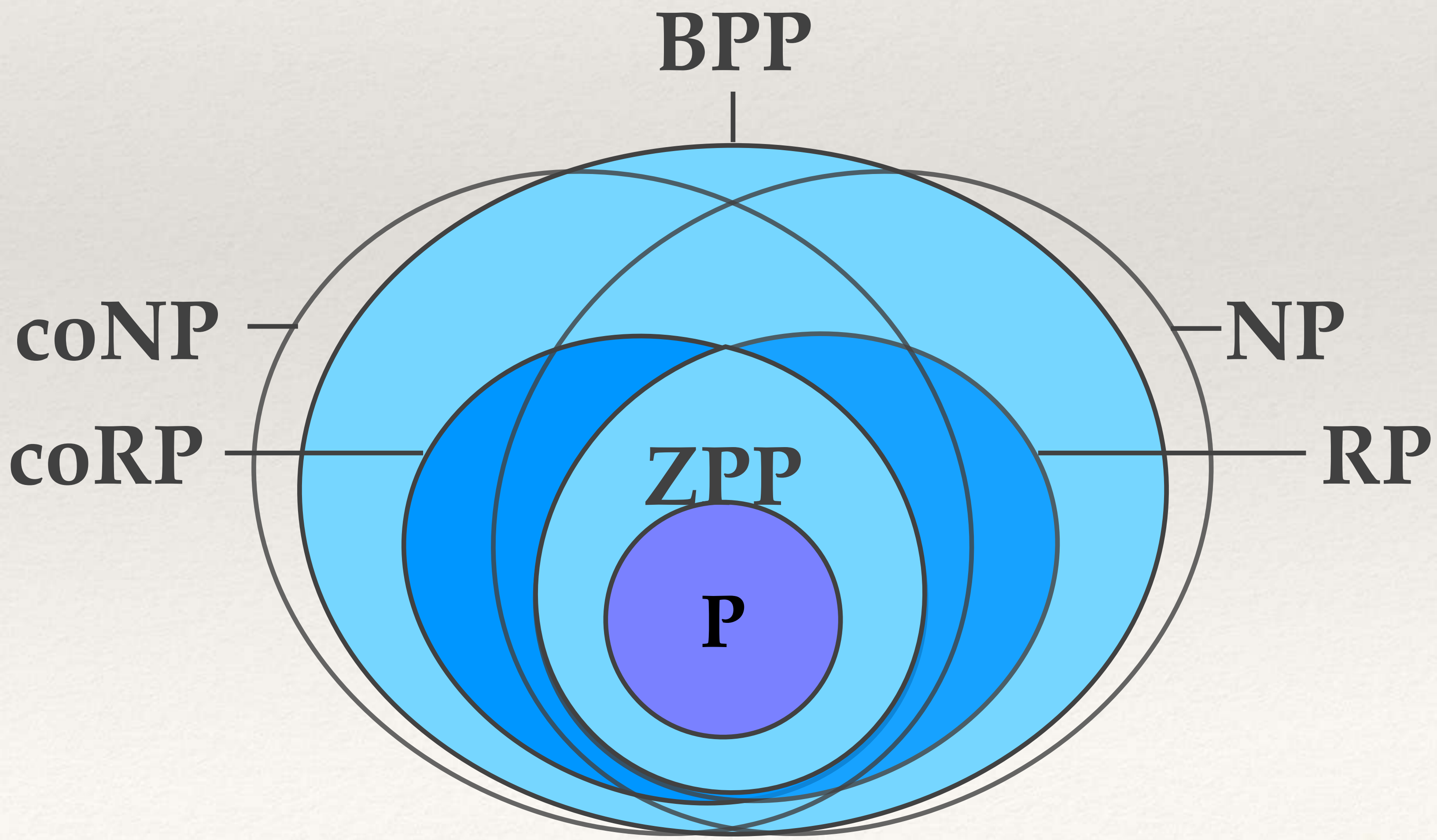
- Both **RP** and **coRP** are included in **BPP**

  (if you make a mistake with prob. 0, then this prob. is ≤1/3!)

- **BPP** is closed under complements: **BPP=coBPP**

  (easy)

- … but what is the relation between **BPP**, **NP**, **coNP**, etc.?

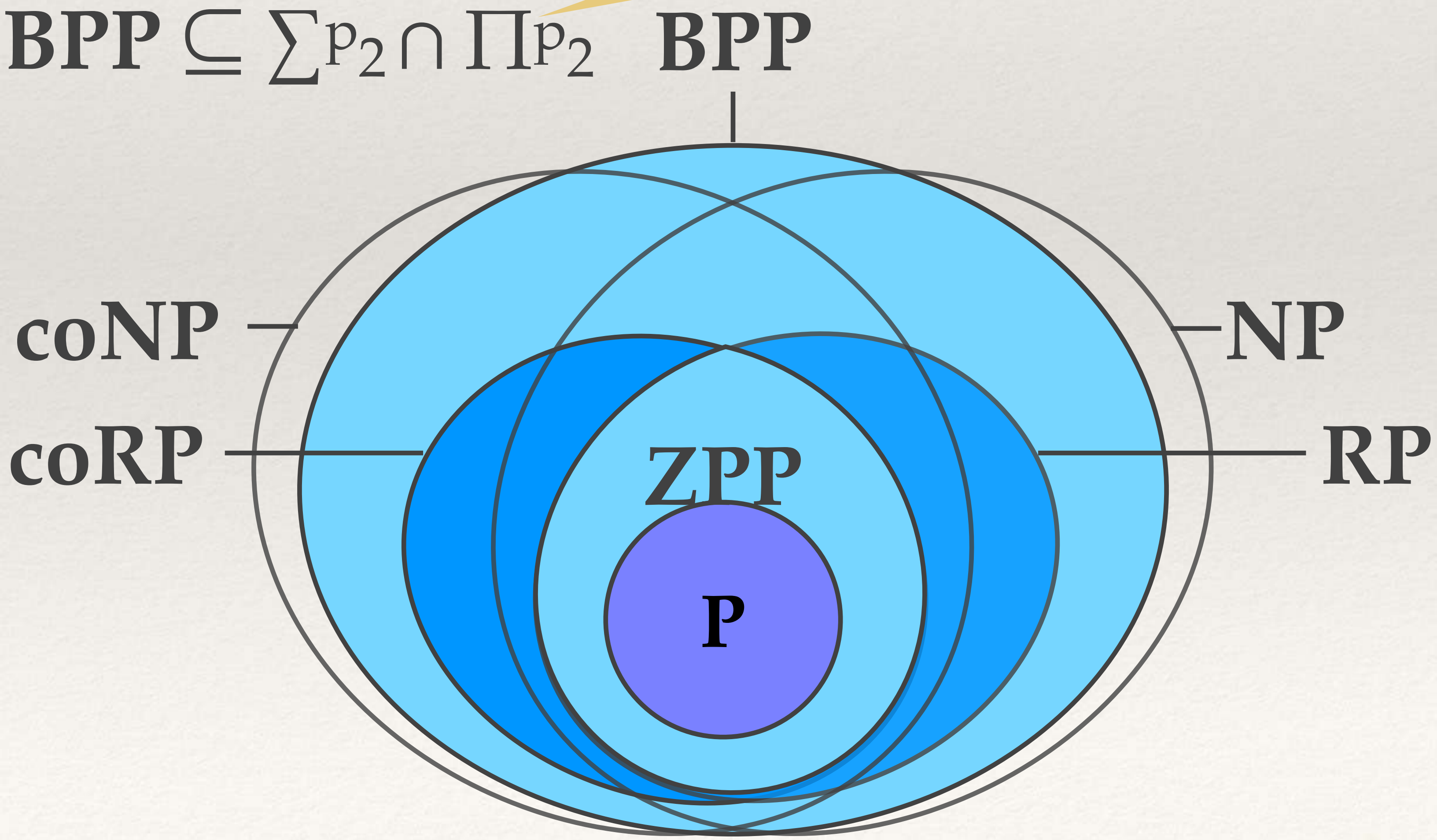


BPP cannot be too large

- It is unknown whether **BPP** ⊆/⊇ **NP** (eqv., **coNP**)
  … but we will see that **BPP** ⊇ **NP** would have
  drastic (and unlikely) consequences

We start with this one

- We will also see that **BPP** ⊆ $\Sigma^p_2 \cap \Pi^p_2$
- … no significantly better result known! although some believe **BPP**=**P**.



The Sipser-Gács-Lautemann Theorem



http://lpcs.math.msu.su/~ver/photo_album/Collegues/lautemann+allender+wagn

https://gravatar.com/avatar/dc36e666740ff9480eb738e556c887a4?s=200

https://upload.wikimedia.org/wikipedia/commons/thumb/3/34/MIT-Science_Sipser_Michael.jpg/440px-MIT-Science_Sipser_Michael.jpg

The Sipser-Gács-Lautemann theorem

- **Theorem (Sipser-Gács-Lautemann, Prop. 1.24.)** **BPP** $\subseteq \Sigma^{p}_{2} \cap \Pi^{p}_{2}$.
- *Proof sketch.*
  It is enough to prove **BPP** $\subseteq \Sigma^{p}_{2}$.
  Proceeds by **derandomization**.
  In order to do so, we will to prove the **existence** of something
  Funnily, this will involve Erdös' **probabilistic method.**

Of course: Σ^{p}_{2} is a non-randomized class…

$\Sigma^{p}_{2} = \exists \cdot$ **coNP**
$(= \exists \cdot \forall \cdot \mathbf{P})$

To prove that $\exists\, t, P(t)$,
just show that $\Pr_t(P(t)) \neq 0$, or
equivalently that $\Pr_t(\neg P(t)) < 1$

Lautemann's trick

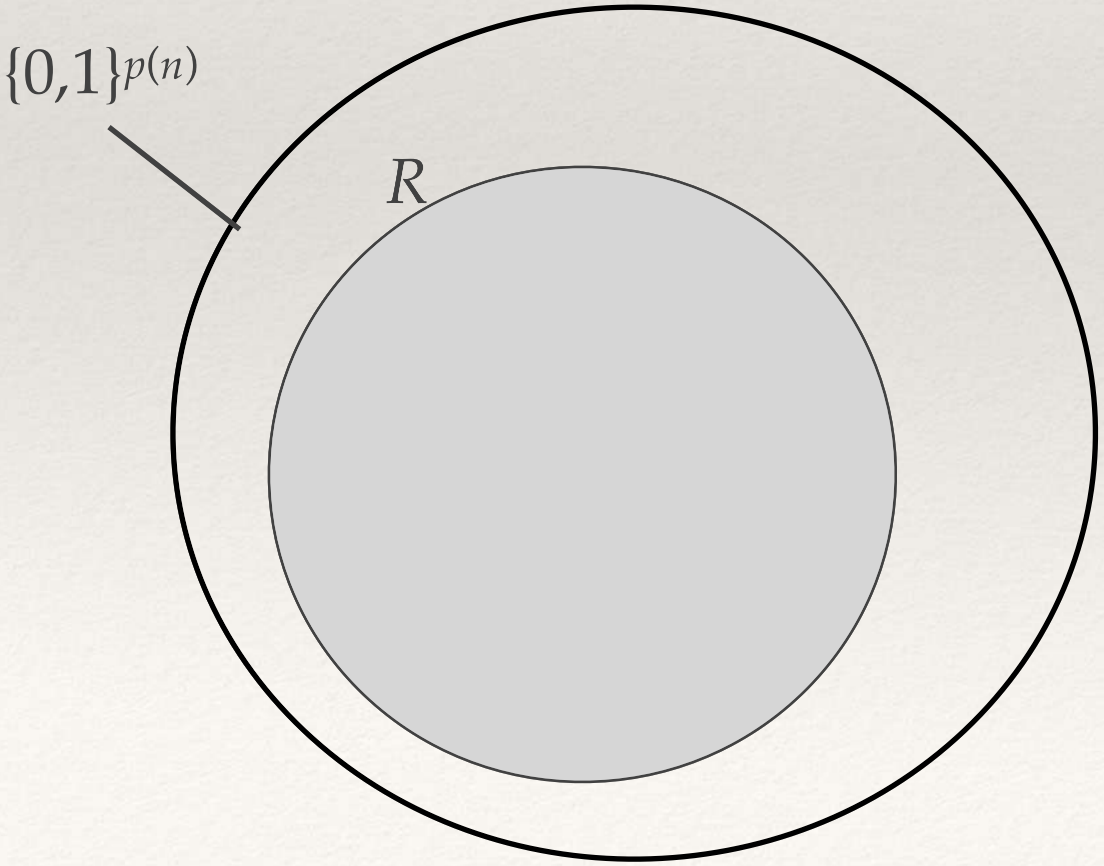
A language L is in **BPP(ε)** and only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):

if $x \in L$ then $\Pr_r$ [$\mathcal{M}(x,r)$ accepts] $\geq 1-\varepsilon$

if $x \notin L$ then $\Pr_r$ [$\mathcal{M}(x,r)$ accepts] $\leq \varepsilon$

error $\varepsilon = 1/2^n$

- Let $L \in$ **BPP**, decided with error
  $\varepsilon = 1/2^n$ (not 1/3)
  in polytime $p(n)$
- Fix x. Then $R = \{r \in \{0,1\}^{p(n)} \mid \mathcal{M}(x,r) \text{ accepts}\}$ is



either **huge**, if $x \in L$

(covers a proportion
$\geq (1-1/2^n)$ of the whole space)

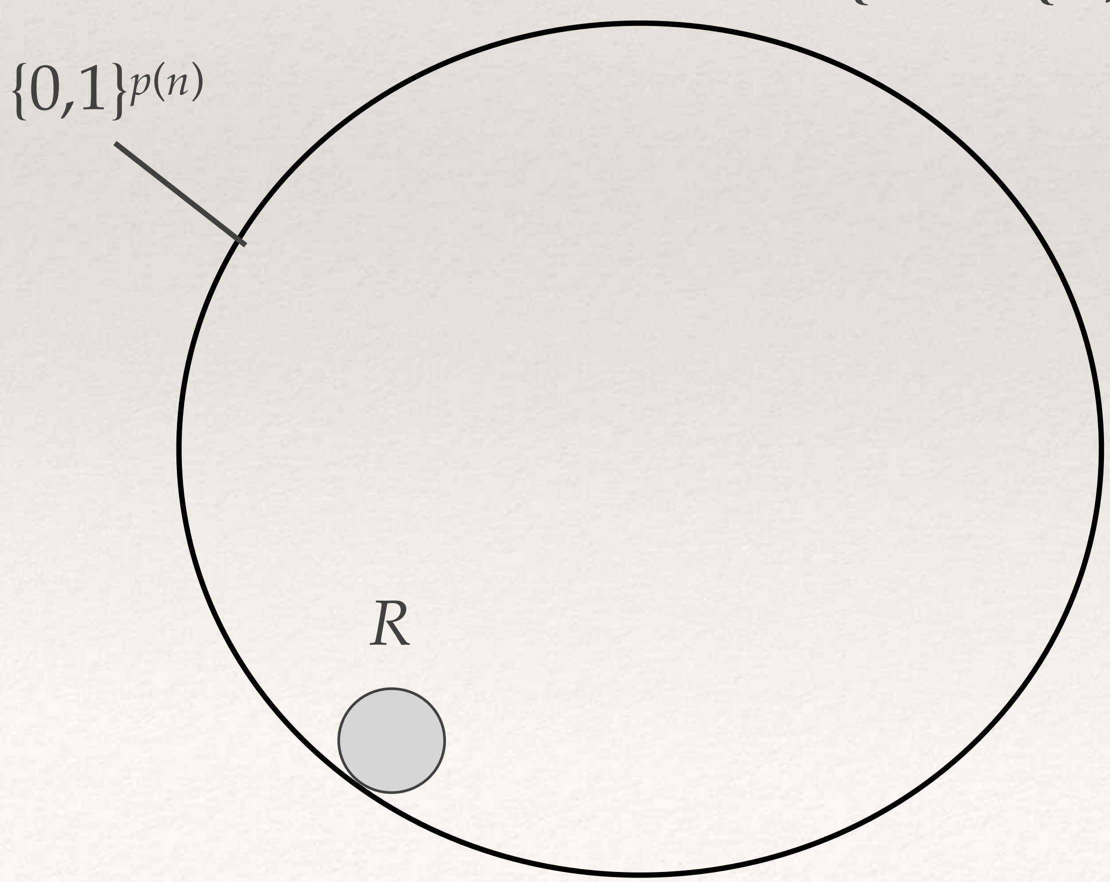
Lautemann's trick

- Let $L \in \mathbf{BPP}$, decided with error
  $\varepsilon = 1/2^n$ (not $1/3$)
  in polytime $p(n)$

> A language L is in $\mathbf{BPP}(\varepsilon)$ nd only if there is a **polynomial-time** TM $\mathcal{M}$ such that for every input x (of size n):
>
> if $x \in L$ then $\Pr_r\,[\mathcal{M}(x,r)$ accepts$] \geq 1-\varepsilon$
>
> if $x \notin L$ then $\Pr_r\,[\mathcal{M}(x,r)$ accepts$] \leq \varepsilon$

error $\varepsilon = 1/2^n$

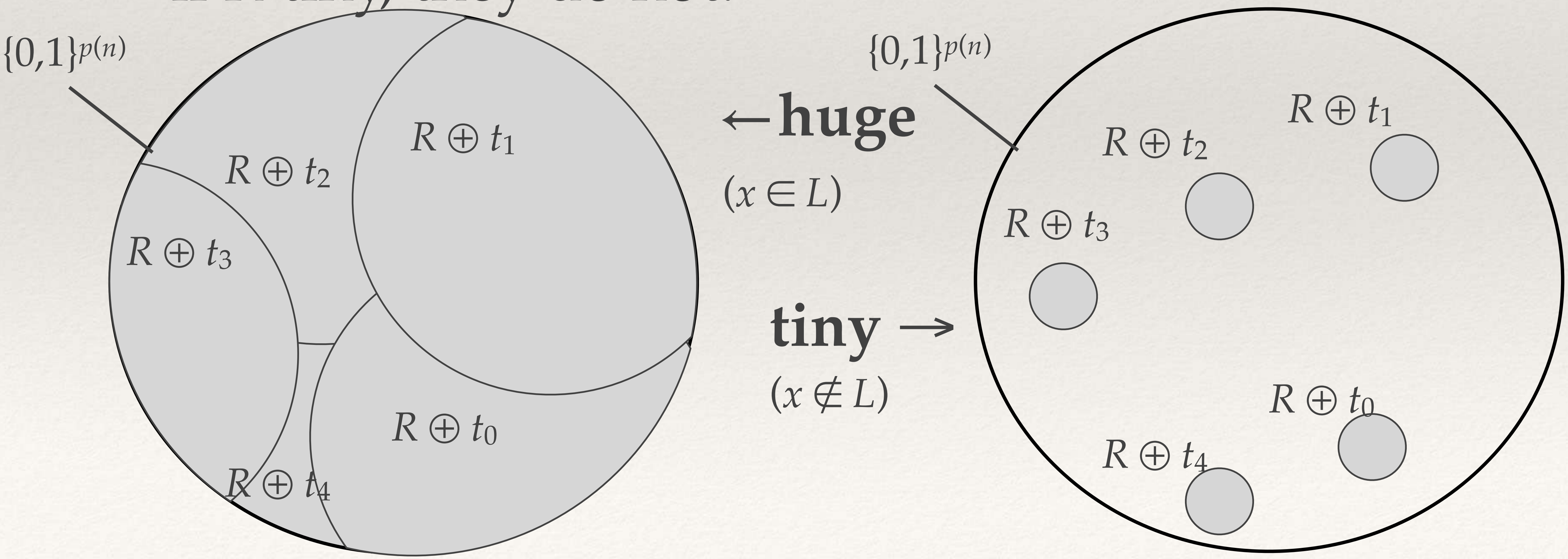
- Fix x. Then $R = \{r \in \{0,1\}^{p(n)} \mid \mathcal{M}(x,r)$ accepts$\}$ is



or **tiny**, if $x \notin L$
(covers a proportion $\leq 1/2^n$ of the whole space)

Lautemann's trick

- $R = \{r \in \{0,1\}^{p(n)} \mid \mathcal{M}(x,r) \text{ accepts}\}$ is **huge** or **tiny**
- We claim there are **translations** $R \oplus t_i$ of R such that:
  — if R huge, then the translations cover the whole space
  — if R tiny, they do not.



Translations?

- The computer science view:

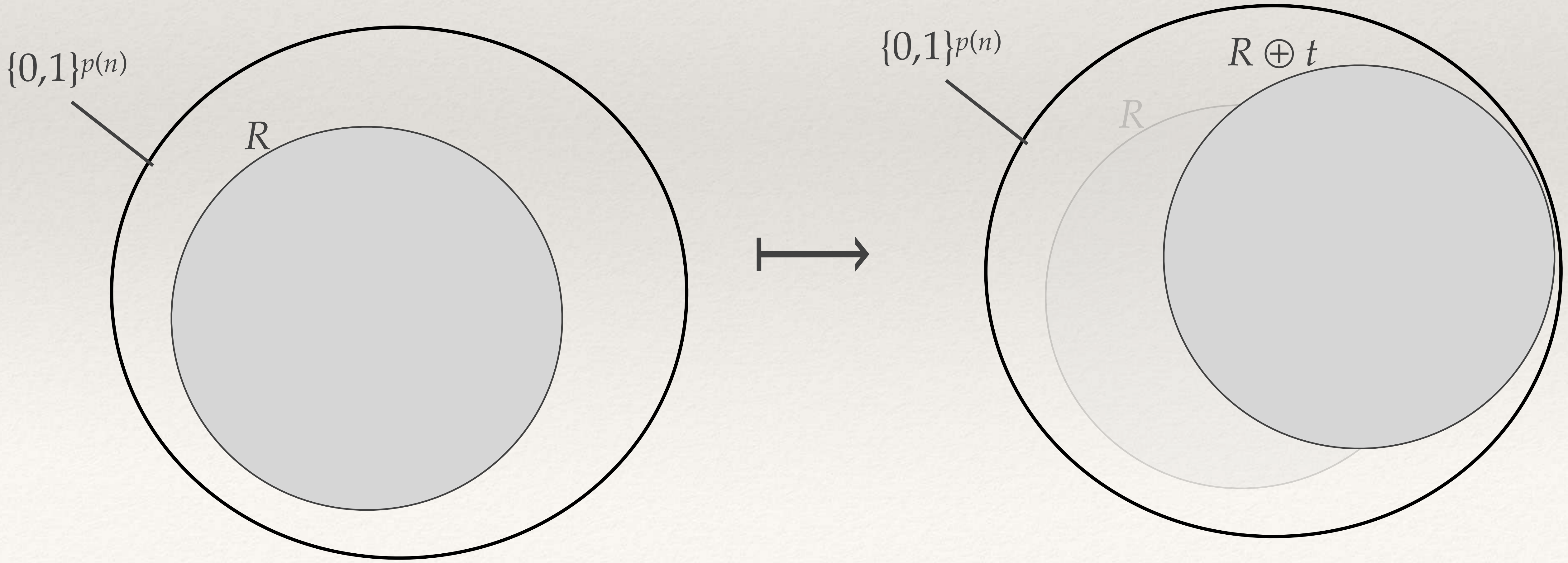
$\oplus$ is **bitwise exclusive-or**

r	0 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 1 0 0 0 0 1 1
t	1 0 1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 0 1 1
$r \oplus t$	1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 1 0 1 0 0 0

- $$R \oplus t = \{r \oplus t \mid r \in R\}$$

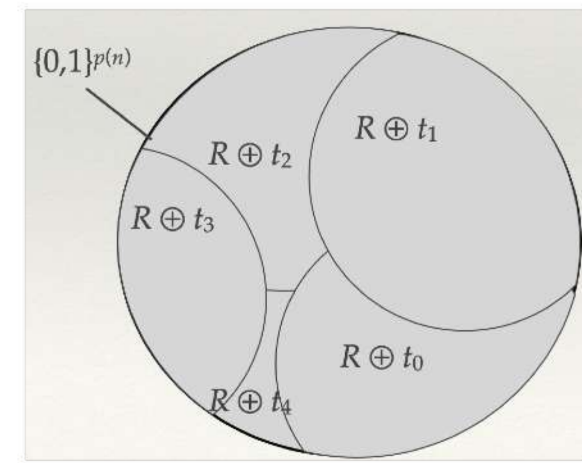
Translations?

- The algebraist's view: $\{0,1\}$ is the **field** $\mathbb{Z}/2\mathbb{Z}$,
  - — exclusive or $\oplus$ is **addition (mod 2)**
  - — $\{0,1\}^{p(n)}$ is a $p(n)$-dimensional **vector space**
  - — and translation $R \oplus t = \{r \oplus t \mid r \in R\}$ is:



The huge case (1/3)

- Assume card $R \geq (1-1/2^n)2^{p(n)}$ (« R is huge »)



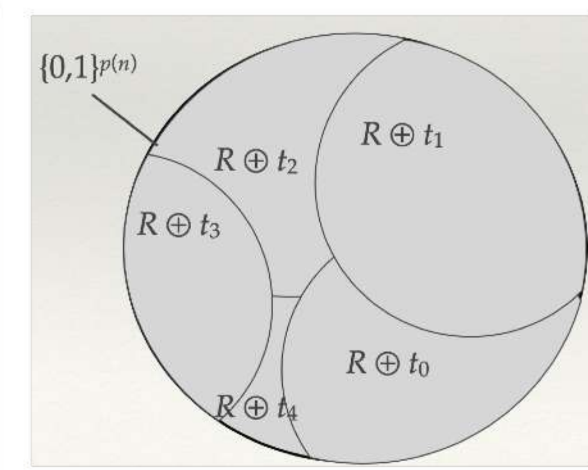
- **Claim.** $\exists\, t_0, \ldots, t_{\lceil m/n \rceil}$ ($m{=}p(n)$) such that $R \oplus t_0, \ldots, R \oplus t_{\lceil m/n \rceil}$ cover $\{0,1\}^m$.
- By the **probabilistic method**. Let $\underline{t}{=}t_0, \ldots, t_{\lceil m/n \rceil}$.
- $\Pr_{\underline{t}}(R \oplus t_0, \ldots, R \oplus t_{\lceil m/n \rceil}$ does **not** cover $\{0,1\}^m)$
- $= \Pr_{\underline{t}}(\exists r, r \notin R \oplus t_0$ and … and $r \notin R \oplus t_{\lceil m/n \rceil})$
- $\leq \sum_r \Pr_{\underline{t}}(r \notin R \oplus t_0$ and … and $r \notin R \oplus t_{\lceil m/n \rceil})$

Sum bound: $\Pr(\exists\ldots) \leq \sum \Pr(\ldots)$

Oh yes, that is a sum of $2^{p(n)}$ terms here!

The huge case (2/3)

- Assume card $R \geq (1-1/2^n)2^{p(n)}$ (« R is huge »)



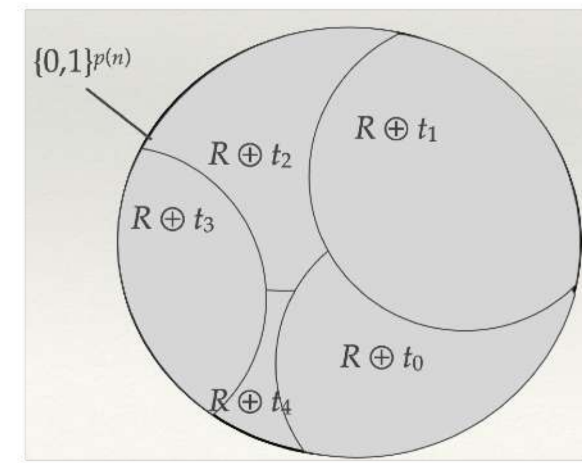
- **Claim.** $\exists\, t_0, \ldots, t_{\ulcorner m/n \urcorner}$ $(m{=}p(n))$ such that $R \oplus t_0, \ldots, R \oplus t_{\ulcorner m/n \urcorner}$ cover $\{0,1\}^m$.
- $\Pr_{\underline{t}}(R \oplus t_0, \ldots, R \oplus t_{\ulcorner m/n \urcorner}$ does **not** cover $\{0,1\}^m)$
- $\leq \sum_r \Pr_{\underline{t}}(r \notin R \oplus t_0$ and … and $r \notin R \oplus t_{\ulcorner m/n \urcorner})$ (from last slide)
- $= \sum_r \prod_{i=0}^{\ulcorner m/n \urcorner} \Pr_{\underline{t}} (r \notin R \oplus t_i)$

(independence)

- $= \sum_r \prod_{i=0}^{\ulcorner m/n \urcorner} \Pr_{\underline{t}} (r \oplus t_i \notin R)$

($r{\in}R{\oplus}t$ iff $r{\ominus}t{\in}R$… but $\oplus{=}\ominus$ mod 2)

The huge case (3/3)



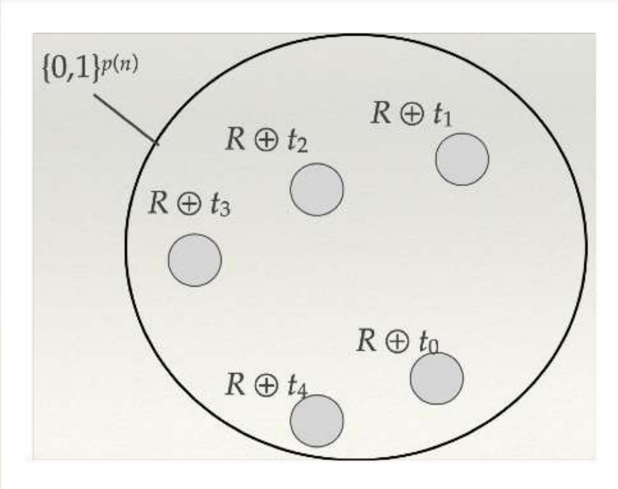
- Assume card $R \geq (1\text{–}1/2^n)2^{p(n)}$ (« R is huge »)
- **Claim.** $\exists\, t_0, \ldots, t_{\ulcorner m/n \urcorner}$ ($m{=}p(n)$) such that
  $R \oplus t_0, \ldots, R \oplus t_{\ulcorner m/n \urcorner}$ cover $\{0,1\}^m$.
- $\Pr_{\underline{t}}(R \oplus t_0, \ldots, R \oplus t_{\ulcorner m/n \urcorner}$ does **not** cover $\{0,1\}^m)$
- $\leq \sum_r \prod_{i=0}^{\ulcorner m/n \urcorner} \Pr_{\underline{t}} (r \oplus t_i \notin R)$ (from last slide)
- $= \sum_r \prod_{i=0}^{\ulcorner m/n \urcorner} \Pr_t (t \notin R)$

  ($t_i \mapsto t \stackrel{\text{def}}{=} r \oplus t_i$ bijection,
  preserves cardinalities)
- $\leq 2^m (1/2^n)^{\ulcorner m/n \urcorner + 1} \leq 1/2^n < 1$ (at least if $n{\neq}0$). Done! □

The tiny case

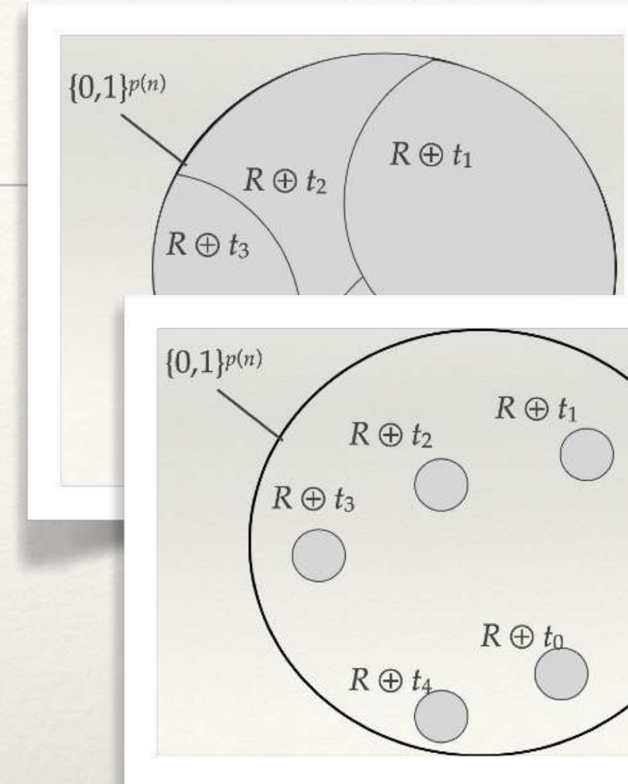
if $n \geq n_0$

- Assume card $R \leq (1/2^n)2^{p(n)}$ (« R is tiny »)
- **Claim.** $\forall\, t_0, \ldots, t_{\lceil m/n \rceil}$ $(m=p(n))$,
  $R \oplus t_0, \ldots, R \oplus t_{\lceil m/n \rceil}$ does **not** cover $\{0,1\}^m$.



- card $(\bigcup_{i=0}^{\lceil m/n \rceil} R \oplus t_i) \leq (\lceil m/n \rceil + 1)\,(1/2^n)2^{p(n)}$
  $= O(\text{poly}(n)/2^n)\; 2^{p(n)}$
- **strictly smaller** than card $\{0,1\}^m = 2^{p(n)}$
  … if n large enough (say $n \geq n_0$). ☐

Testing huge vs. tiny



- $R \oplus t_0, \ldots, R \oplus t_{\lceil m/n \rceil}$ covers $\{0,1\}^m$ iff:
  $\forall r, r \in R \oplus t_0$ or … or $r \in R \oplus t_{\lceil m/n \rceil}$
- iff: $\forall r, r \oplus t_0 \in R$ or … or $r \oplus t_{\lceil m/n \rceil} \in R$
- (Now remember that $R = \{r \in \{0,1\}^{p(n)} \mid \mathcal{M}(x,r)$ accepts$\}$.)
  iff: $\forall r, \mathcal{M}(x, r \oplus t_0)$ or … or $\mathcal{M}(x, r \oplus t_{\lceil m/n \rceil})$ accepts.
- If $x \in L$, $\exists\, t_0, \ldots, t_{\lceil m/n \rceil}$,
  $\forall r, \mathcal{M}(x, r \oplus t_0)$ or … or $\mathcal{M}(x, r \oplus t_{\lceil m/n \rceil})$ accepts.
- If $x \notin L$, such $t_0, \ldots, t_{\lceil m/n \rceil}$ do not exist (for $n \geq n_0$).

The algorithm

- Hence, for every x of size $n \geq n_0$,

  $x \in L$ iff $\exists\, t_0, \ldots, t_{\ulcorner m/n \urcorner}$,

  $\forall r$, $\mathcal{M}(x, r \oplus t_0)$ or … or $\mathcal{M}(x, r \oplus t_{\ulcorner m/n \urcorner})$ accepts.

  polytime (note $\ulcorner m/n \urcorner = \ulcorner p(n)/n \urcorner = \text{poly}(n)$)

- For $n < n_0$, **tabulate** the answers.
- Hence L is in Σ^p_2.
- Since L is arbitrary in **BPP**, **BPP** $\subseteq \Sigma^p_2$. □

The Sipser-Gács-Lautemann theorem

- **Theorem (Sipser-Gács-Lautemann, Prop. 1.24.)**
  $\mathbf{BPP} \subseteq \Sigma^p_2 \cap \Pi^p_2$.
- *End of proof.*
  We have shown $\mathbf{BPP} \subseteq \Sigma^p_2$.
- Now $\mathbf{BPP} = \mathbf{coBPP} \subseteq \mathbf{co}\Sigma^p_2 = \Pi^p_2$. □

Useful **Lemma.** Given two classes C_1, C_2,
if $C_1 \subseteq C_2$ then $\mathbf{co}C_1 \subseteq \mathbf{co}C_2$.
(Let $L \in \mathbf{co}C_1$. The complement of L is in C_1 hence in C_2.)

No, $\mathbf{co}C$ is **not** the complement of C.
It is the class of complements of languages in C.

Next time…

P/poly

- We will introduce a strange complexity class defined by **families of circuits**:
  P/poly
- Studying it, we will eventually show that **BPP** probably does **not** contain **NP**
  … otherwise **PH** would collapse at level 2!