<u>6 May 2024</u>	Prozvam	Checking
Plan Plan Reserves	.       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .	.       .
* Announcements		.       .
* Matrix Multiplicati		.       .
.       .	.       .	.       .
		·       ·
.       .	.       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .	.       .
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

Τn	4820	·       ·
· · · · · · · ·	Designed Algorithm.	s for computational problems
	Proof of Correc	ctness essential
 	· · · · · · · · · · · · · · · · · · ·	.       .
· · · · · · ·	· · · · · · · · · · · · · · · · · · ·	.       .
 	· · · · · · · · · · · · · · · · · · ·	.       .
· · · · · · ·		·       ·
· · · · · · ·	· · · · · · · · · · · · · · · · · · ·	<ul> <li></li></ul>
· · · · · · ·	· · · · · · · · · · · · · · · · · · ·	·       ·
.       .       .       .       .         .       .       .       .       .       .         .       .       .       .       .       .         .       .       .       .       .       .		.       .

 $I_{n}$  4820 \* Designed Algorithms for computational problems La Proof of Correctness essential Outside of 4820 \* May encounter programs w/ bugs. Can we make use of programs that may make mistakes?

$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	gram Chec	hing		  
	en in a son	m P supposed	(as a blach-box) to compute function f.	.       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .         .       .       .       .
· · · · · · · · · · · · · · · · · · ·	and in put			· · · · ·
· · · · · · ·	.       .			  
· · · · · ·	.       .	.       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .       .         .		· · · · ·
· · · · · ·		.       .		

Program Cheching.
Given
* a program P (as a black-box)
that is supposed to compute function f.
* an input x
Check: Does $x \rightarrow (P) \rightarrow Z = f(x)$ ?
* If $P(x) = f(x)$ , accept
* If $P(x) \neq f(x)$ , reject with high probability.

Check?	Does		$= \int (x) \frac{1}{6} + \frac{1}{6$
· · · · · · · · · · · · · · · · · · ·	$P(x) = f(x)$ $P(x) \neq f(x)$	)	with high probability.
$(\sqrt{2}) e^{-e^{-e^{-e^{-e^{-e^{-e^{-e^{-e^{e^{e^{e^{e^{e^{e^{e^{e^{e^{e^{e^{e^{e$	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
× Check	Shonald Kunia	faster than	Compatilizer f
* Check	should use	vand omness	
* Check	should use	vandomness	
× Check	Should use	vand omness	

Announcements
* FINAL EXAM. 16 May 2024, 7p.
Lo Watch Ed for any announcements
* OH. Check Mu online calendar.
TODAY: My OH @ 2P
* Fill out Course Evals! by May 10th
·       ·
* Fill out Conve Evals! by May 10th

• •	Na	t t		, , ,	· ·	M	لم	_ ( -	ti	ρl	r , C		f-2	י 20 1	) }	•	• •	• •	•	•	•	•	• •	•	•	· ·	•	•	•	••••	•	•	•	· ·	•	•
	• •	• •	•	•				•			•							, ,		٠		٠											٠	• •		
	 • •			•				٠	• •	• •	٠	•	٠	٠	٠	٠	• •	• •			٠	٠			•						٠		•	• •		٠
	 • •		•	•	• •	•	•	•		•••	•	$\bigwedge$		•	•		>				•	1	<u> </u>	•	•	• •	•	•	•	• •	•	•	•	• •	•	•
	 						•									ſ	$\supset$		•				<u> </u>					•				•	•			
	 					•													•						•											
	 			•				•	•				٠			•													•				*	• •		
• •	 • •	• •		٠	• •	٠	٠	0	• •	• •	٠	٠	۰	٠		٠	• •		٠	٠	٠		• •	٠	٠	• •		٠		• •	٠	٠	٠	• •	٠	٠
	 • •	• •		•	• •	٠		•	• •		•	•	•	٠	٠	•					٠	•		•					•				٠	• •	٠	٠
• •	 • •	• •	٠	٠	• •	٠	•	٠	• •	• •	•	•	•	•	٠	•	• •	• •	•	*	٠	٠	• •	•	*	• •	٠	•	٠	• •	•	•	*		*	•
	 • •		•	•		•		•			•	•							•	•		•		•	•		•		•			•	•		•	
	 		٠												•						٠	•			٠											
	 • •	• •	٠	*	• •	*	•	0	• •	• •	•	•	*	٠	٠	•	• •		٠	+	٠	٠	• •	•	*	• •	٠	•	٠	• •	٠	•	*	• •	٠	٠
	 		•	•		٠		•	• •		٠		٠	٠	٠	٠	• •	• •	•	•	٠	•			٠	• •	٠		٠				•	• •	٠	٠
	 	• •	٠	٠	• •	۰	٠	0	• •	• •	•	٠		•	٠	•	• •		۰	۰	٠	٠	• •	٠	۰	• •		٠		• •	٠	٠	٠	• •		•
• •	 • •	• •	•	•	• •	•	•	•	• •	• •	•	•	•	•	•	•	• •	• •	•	•	•	•	• •	•	•	• •	•	•	•	• •	•	•	•	• •	•	•
	 												*																							
	 	• •	٠	٠	• •	٠	٠	0	•	• •	•	•		٠			• •						• •		٠	• •		٠			٠	٠		• •	٠	٠
	 • •	• •		•				•						•															•				٠	• •		
	 	• •	٠	٠	• •	٠	•		• •	• •	٠	٠		٠	٠	•	• •		٠	٠	٠	٠	• •	٠	٠	• •	٠	٠		• •	•	•	٠	• •	٠	•
• •	 • •	• •			• •			•	• •				٠	•		•	• •		•			•				• •	•		•	• •			•	• •		
	 		•	•		•	•	•			•	•	•	•	•				•	•	•	•			•		•	•	•			•	•		•	•
	 					٠																											•			
	 • •		٠	•				٠							٠				•		*	٠					*		•				•			
• •	 	• •	٠	•		•			• •		•		٠	٠	٠	•	• •	• •	•		٠	٠	• •		•	• •	٠		٠	• •	٠		•	• •	•	٠
	 	• •	•	٠	• •	٠	•	٠	•	• •	•		•	•			• •		٠	٠	•	٠	• •	٠	٠		•	٠	•		٠	•	٠	• •	٠	•
• •	 • •	• •	•			•			•		*			•		•	• •		•			•	• •		•	• •	•		•	• •			•	• •	•	
• •	 	• •	٠		• •	•		•	• •		٠	•	•	•	•	•	• •		•			•	• •	٠	•	• •	•	•	•	• •	•		•	• •	•	

Matrix Multiplication  $B_{11} = B_{12} = B_{17}$  $\Delta_{1}^{\alpha} = \left[ \begin{array}{ccc} A_{11} & A_{12} & --- & A_{11} & A_{12} \\ A_{21} & A_{21} & A_{21} & A_{22} \\ A_{21} & A_{21} & A_{22} & A_{22} \\ A_{21} & A_{22} & A_{22} & A_{22} \\ A_{21} & A_{22} & A_{22} \\ A_{22} & A_{22} \\ A_{22} & A_{22} &$ An. - - Ann J Bni  $\left(\begin{array}{c} \left\langle \widehat{A}_{1}, B_{1} \right\rangle & \left\langle \widehat{A}_{1}, B_{2} \right\rangle & \sim & \left\langle \widehat{A}_{1}, B_{n} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{1} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle & \left\langle \widehat{A}_{2}, B_{2} \right\rangle \\ \left\langle \widehat{A}_{2}, B_{2} \right\rangle$  $A \xrightarrow{i} A \xrightarrow{i}$  $\langle \hat{A}_{h}, B_{i} \rangle$  $\langle \widetilde{A}_{n}, B_{n} \rangle$ where  $\langle \hat{A}_{i}, B_{j} \rangle = \sum_{i,j}^{k} A_{ijk} \cdot B_{ij}$ 

Matrix Multiplication
A.B. // involves nº inner products
$\sum_{k=1}^{n} A_{ik} + B_{ik}$
Naive Algo. $O(n^3)$ operations
Fastest Algo. O(n <sup>w</sup> ) operations
where (2) < 2.373
·       ·
·       ·

Cheching Matrix Mult
Given: Program P, nxn matrices A, B
$\sum_{i=1}^{n} \left( \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right) + \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right) + \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right) + \left( A_{i} \right)^{i} B_{i} \right) + \left( A_{i} \right$
supposedly equal to A.B.
Can we chech that
$C = A \cdot B$
without running Matrix Melt?

Matrix - Vector Multiplication Naire Algo O(n<sup>2</sup>) operations Can we check Matrix Mult using calls to Matrix-Vector Milt?

$f_{z}$	$B = \left\{ \begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 $	.       .
		$ \begin{array}{c} \begin{array}{c} \\ \\ \\ \\ \end{array} \end{array} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ $

Ideas?  $\mp f = A \cdot B, \quad \text{then}$ for all v γ, . . . MJ

Random	"spot checks"	Caha	Frievalds	
<u>Given</u> A	B, B, and C	supposedly	equal to	A = B
.       .	.       .	· · · · · · · · · · ·	.       .	
· · · · · · · · · · · ·	·       ·	· · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · ·
· · · · · · · · · · · ·	.       .	· · · · · · · · · · ·	· · · · · · · · ·	.     .     .     .     .     .     .       .     .     .     .     .     .     .       .     .     .     .     .     .     .
· · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · ·	 
· · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · ·
· · · · · · · · · · · · ·		· · · · · · · · · · ·		· · · · · · · · ·
·       ·		· · · · · · · · · · ·		· · · · · · · · ·

Random "spot checks" (aka Frievalds' Algo)
Given A, B, and C supposedly equal to A.B
· · · · · · · · · · · · · · · · · · ·
- sample r <- ZO,13 <sup>h</sup> uniformly at random
$$ $$ $$ $$ $$ $$ $$
$ \begin{array}{c} & & & \\ & & & & \\ & & & \\ & & & & & \\ & & & & \\ & & & & \\ & & & & & \\ & & & & \\ & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & $
$\sim$ if $x \neq Z$ , $REJECT$
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·

Random "spot checks" (aka Frievalds' Algo)
Criven A, B, and C supposedly equal to A-B
- sample r < ZO113 <sup>h</sup> uniformly at random
$-\frac{1}{2} + \frac{1}{2} + 1$
$\sim$ if $\times \neq \mathbb{Z}$ , $\mathbb{R} \in \mathbb{J} \in \mathbb{C} \setminus \mathbb{C}$
Claim for every $r \in 20, 13^{n} = (A \cdot B) \cdot r$

(aha Frievalds' Algo) Random "spot checks" Given A, B, and C supposedly equal to A-B Repeat T times. - sample r <= ZO,13<sup>h</sup> uniformly at random  $\begin{array}{c} \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \\ \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \\ \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \begin{array}{c} \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \end{array} \end{array} \xrightarrow{\bullet} \begin{array}{c} \bullet \end{array} \xrightarrow{\bullet} \end{array} \xrightarrow{\bullet} \begin{array}{c} \end{array} \end{array}$  $if \quad x \neq Z$ REJECT ACCEPT

Repeat	fine	S.,	· · · · · · · · · ·	· · · · · · · · · · ·	· · · · ·	
	uple r		20,134	uniformly		random
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	· · · · · · · · · · · · · · · · · · ·	· · · · ·	· · · · · · · · · ·	· · · · · · · · · ·	· · · · ·	· · · · · · · · ·
			· · · · · · · · · ·		· · · · ·	
· · · · · · · · · · ·	y		· · · · · · · · · ·	· · · · · · · · · · ·	· · · · ·	· · · · · · · · ·
	× +	$\frac{1}{2} = \frac{1}{2} + \frac{1}$	REJE		· · · · ·	· · · · · · · · ·
ACCEPT	· · · · · · · ·	· · · · ·	· · · · · · · · ·	· · · · · · · · · · ·	· · · · ·	· · · · · · · · ·
C [a; m]				then the	· · · · · ·	heeleer
· · · · · · · · · · ·	· · · · · · A C		s with	Probalei (i.	ty	

Repeat T time	5		· · · · · · ·	
sample r	- < Zo <sub>1</sub>	zh Juniforn	rly at	random
Let	· · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · ·	· · · · · · · · · ·
		· · · · · · · · · ·	· · · · · · ·	 
$\begin{array}{c c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\$	$A \circ A \circ$			
$if \times \neq 2$		JECT		
ACCEPT	· · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · ·	· · · · · · · · ·
Suppose C = A		· · · · · · · · · · ·	· · · · · · ·	· · · · · · · · ·
What is the	Probability	Checher	r REJE	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

$\Pr_{\mathbf{v} \leftarrow \mathbf{r} \circ \mathbf{v}^{N}} \left[ C \cdot \mathbf{v} \neq \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{v} \right] \geq \frac{1}{2}$	Claim.	$\mathbb{I}_{\mathcal{I}} = \mathbb{I}_{\mathcal{I}} = $		then	
	· · · · · · · · ·	$P_{V} = \{o_{i}, c_{j}\}^{n}$	$\bigcap_{i=1}^{n} \cdot \bigvee_{i=1}^{n} \downarrow \downarrow$	$\begin{bmatrix} A & B & A & A \\ B & A & C \\ A & A & A \\ A & A & A \\ A & A & A \\ A & A &$	$\sum_{i=1}^{n} \sum_{i=1}^{n} \sum_{i$
	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·
	· · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · ·		· · · · · · · · · · · · · · · · · ·
	· · · · · · · · ·		· · · · · · · ·	· · · · · · · · · · · ·	
1       1	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · ·
· ·	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·
					· · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · ·		· · · · · · · · · · · · · · · · · ·
	· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · ·

Claim. If $C \neq A \cdot B$ , then $P_{r} \left[ C \cdot r \neq A \cdot B \cdot r \right]$ $r \in \operatorname{Por}_{r} \left[ C \cdot r \neq A \cdot B \cdot r \right]$		
Corollary. If C = A B, then	.       .       .       .       .       .         .       .       .       .       .       .       .         .       .       .       .       .       .       .         .       .       .       .       .       .       .         .       .       .       .       .       .       .         .       .       .       .       .       .       .	.       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .       .
Pr [ Checker ACCEPTs ]	$\leq \frac{1}{2} + $	$\overline{\tau}$
.       .	.     .     .     .     .     .       .     .     .     .     .     .       .     .     .     .     .     .       .     .     .     .     .     .	<td< td=""></td<>
.       .	.     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .       .     .     .     .     .	.       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .         .       .       .       .       .       .       .       .       .       .       .
.       .	.     .     .     .     .     .       .     .     .     .     .     .       .     .     .     .     .       .     .     .     .     .	.       .

Claim. If C = A B, then  $P_{V} = A \cdot B \cdot C$ Pf By the Principle of Deferred Decisions.

Claim. If $C \neq A \cdot B$ , then $ \begin{array}{l} P_{v} \left[ C \cdot v = A \cdot B \cdot v \right] \geq \frac{1}{2} \\ v \leftarrow \tau_{0},\tau_{1}^{n} \end{array} $
Pf By the Principle of Deferred Decisions.
If $C \neq A \cdot B$ , then there exists $i, j$ s.t.
$C_{i} + \frac{1}{2} + \frac{1}{2$
$\Rightarrow$ the jth entry of $v$ is crucial.
·       ·

$C_{ij} \neq C_{ij} \neq C_{ij} = \frac{1}{2} + \frac{1}{2}$														
		$\sum_{k=1}^{n} C_{ik} \cdot I$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\sum_{k=1}^{N} (A \cdot B)_{ik} \circ V_{k}$										

$C_{\dot{v}} \neq C_{\dot{v}} + C_{\dot{v}} $
Let $U = \sum_{k=1}^{n} C_{ik} \cdot r_{k}$ $V = \sum_{k=1}^{n} (A \cdot B)_{ik} \cdot r_{k}$
Imagine we "defer" flipping the jth bit of r until all others have been flipped.
$Y_1 / Y_2 / \cdots / Y_{j-1} / Y_{j+1} / \cdots / Y_n$ $(x_1 / y_2 / \cdots / y_n)$

$C_{\dot{i}} = \left( A_{\dot{i}} + B_{\dot{i}} \right)_{\dot{i}} = \left( $
Let $U = \sum_{k=1}^{n} C_{ik} \cdot v_{k}$ $V = \sum_{k=1}^{n} (A \cdot B)_{ik} \cdot v_{k}$
Imagine we "defer" flipping the jth bit of r until all others have been flipped.
$\gamma_{1}, \gamma_{2}, \dots, \gamma_{j-1}, \gamma_{j+1}, \dots, \gamma_{N}$
$\mathcal{U}_{ij} = \sum_{k \neq j}^{2} C_{iu} \cdot v_{u}$ $\mathcal{V}_{ij} = \sum_{k \neq j}^{2} (A \cdot B)_{ik} \cdot v_{u}$

 $\begin{array}{c} \begin{array}{c} C \\ C \\ C \\ \end{array} \end{array} \end{array} \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ C \end{array} \right) \xrightarrow{} \left( \begin{array}{c} C \\ \end{array} \end{array}$  $\mathcal{U} = \mathcal{U}_{j} + \mathcal{C}_{j} \cdot v_{j} + (\mathcal{A} \cdot \mathcal{B})_{j} \cdot v_{j}$ What is Pr[U7V] ? Vjezons

 $\mathbb{C}_{\mathbf{x}}^{\mathbf{x}} \stackrel{\mathbf{x}}{\to} \stackrel{\mathbf{x}}{\to}$ =  $(A \cdot B)_{ij} \cdot (A \cdot B)_{ij}$  $M = M_{ij} + C_{ij} \cdot v_j$  $\frac{Case}{\sqrt{3}} = \sqrt{3}$  $P_{r}\left[\mathcal{U}_{j}\right] = P_{r}\left[\mathcal{U}_{j}\right] = \left[\mathcal{U}_{j}\right] = \left[\mathcal{U}_{j$ Vjetor

 $C_{ij} = \left[ \begin{array}{c} c \\ c \\ c \end{array} \right]_{i} = \left[ \begin{array}{c} c \\ c \end{array} \right]_{i} = \left[ \begin{array}[ c \\ c \end{array} \right]_{i} =$  $= (A \cdot B)_{ij} + (A \cdot B)_{ij}$  $M = M_{ij} + C_{ij} \cdot v_{j}$ What is Pr[U7V]?  $P_{r}\left[\mathcal{U},\neq \mathcal{V}\right] = P_{r}\left[\mathcal{V}_{j}=1\right] = \left[P_{r}\right] = \left[P_{r}\right] = \left[P_{r}\right]$  $\frac{Case}{2} = \sqrt{2}$  $\Pr\left[\mathcal{U}\neq\mathcal{V}\right]\geq\Pr\left[\mathcal{C}_{j}=0\right]=$ Vjefor<sup>z</sup>

So. * Checker	always $ACCEPT_s$ when $C = A \cdot B$
XChecher	REJECT, w.p. $l - \frac{1}{2}$ when $C \neq A \cdot B$
* Checker	runs 37 Matrix-Vector mults.
.       .	
.       .	
	.       .

$S_{2}$ . * Checker always ACCEPTS when $C = A \cdot B$
* Checker REJECT, W.P. $I - \frac{1}{2^{T}}$ when $C \neq A \cdot B$
* Checker runs 37 Matrix-vector mults.
$e \cdot g \cdot \overline{1} = 10 \log v \cdot \overline{1}$
- Checker runs in O(n <sup>2</sup> logn) time
- Makes mistake with probability at most 1/n10

•	•	•	•		•			• •	•	٠			•	• •	٠			•		۰	•	•		•	•		• •	•		•	•		•	• •	•	٠	• •	٠
٠	•	٠	•		•					٠	٠	٠	•	• •			•		• •	٠				•	٠	•	• •	٠	•	*	• •	٠	٠	• •		•	• •	•
								• •			0		•	• •					• •		٠	•		•	0		• •			•				• •		٠	• •	٠
	٠	•	•		٠	•	٠	• •	٠	٠	٠		•	• •				٠	• •	٠	٠	•		•	٠	•	• •		٠	•			٠	• •	•	٠		•
•		•				•	•		•				•	• •				٠				•		•		•	• •		٠	•					•	٠		
								• •					•	• •					• •		٠	•		•			• •			•			٠					٠
	•	•	•		•		•		•	•	٠		•	• •				٠	• •	•	•			•	٠		• •			•			٠		•			
		•				•							•	• •				•				•		•		•			٠	•					•			
		•	•										•	• •				•			٠	•		•		•				•			٠		•			
•	•	•	•		٠	•	•		٠	٠			•	• •				*	• •	٠		•		•	*	•	• •	•	٠	•			٠		*	٠		
		•											•					•				•		•		•				•					•			
		•	•										•	• •				•						•		•				•			٠		•			
•		•	•		•		•		•		•	•	•	• •		•		•		•				•			• •			•			•	• •	•		• •	
			•										•	• •				•				•		•		•				•					•		• •	
		•	•										•	• •				•						•						•			٠		•			
•	•	•	•	• •	٠		٠		٠	•	•	•	•	• •		٠		٠		٠				•			• •	•		•			•	• •	•		• •	
٠	•	•	•							•		٠	•	• •	•	۰	•	•		٠			• •	•			• •	٠		•		•		• •	•		• •	
٠	٠	•	•	•	٠				٠	٠		٠	•	• •			•	0	• •		*			•	*	•	• •	٠	٠	*	• •	٠	٠	• •		٠	• •	*
٠	٠		• •		٠	•	٠	• •	٠	٠	٠	٠	•	• •	٠	٠	٠			٠	٠	•	• •	•	٠	•	• •	٠	•	•		٠	٠	• •		•	• •	٠
٠	•		•		٠	•		• •		٠		٠	•	• •	٠		٠	0	• •	٠	٠	•		•	٠	٠	• •	٠	٠	•		٠	٠	• •		٠	• •	٠
٠	٠	•	•	•	٠				٠	٠		٠	•	• •			•	0	• •		*	•		•	٠	•	• •	٠	٠	*	• •	•	٠	• •		٠	• •	
٠	•		• •		٠	٠	٠	• •	٠	٠		٠	•	• •	٠	٠	٠			٠	٠	•	• •	•	٠	٠	• •	٠	٠	•		٠	٠	• •		•	• •	٠
٠	•	0	•		٠	•		• •	•	٠		٠	•	• •	•		٠	0	• •		٠	•		•	٠	•	• •	٠	٠	•		٠	٠	• •	0	٠	• •	٠
٠	٠	٠	•	• •	٠	•			٠	٠		•	•	• •					• •		*	•		•	٠	•	• •	٠	٠	*	• •		٠			٠	• •	*
		•	•			•							•	• •			•	•			•	•		•		•		•		•					•			•
•	•	•	• •		•		•		•	•	•	•	•	• •		٠		•	• •	•			• •	•			• •	•		•			•	• •	•		• •	
•	•	•	•	• •	٠	•	٠	• •	٠	٠	•	•	•	• •	٠	٠	•	٠		٠	•			•	•		• •	•		•		•	•	• •	•		• •	
٠	•	٠	•		٠	•		• •	•	٠	٠	٠	•	• •	٠	٠	•	٠			٠			•	٠		• •	٠		•		٠	٠	• •	•		• •	•
•	•	•	•		•		•	• •	•				•	• •				•	• •	•				•			• •			•			٠		•		• •	٠
•	•	•	•	• •	٠		٠		٠	•	•	•	•	• •	•	٠		٠	• •	٠				•	•		• •			•		•	•	• •	•		• •	
	•	•	•		•			• •		•	•		•	• •			•	•			•	•		•		•	• •	•		•			•	• •	•		• •	•
•		•	•		•		•	• •	•	•	•	•	•	• •		•		٠	• •	•				•			• •			•			٠		•		• •	•
•		•	•			•	•		•			•	•	• •			•	•				•		•		•	• •	•	٠	•		•			•		• •	٠
•	٠	•	•		٠	•		• •	٠	٠			•	• •				•	• •		٠	•		•		•	• •	•	٠	•			٠	• •		٠	• •	٠
٠	*	•	•	• •	٠	•	٠	• •	٠	٠	٠	•	•	• •		٠		٠	• •	٠	٠	•		•	٠	•	• •	٠	٠	*	• •		٠		•	٠	• •	•
٠	•		•		٠	٠		• •		٠		٠	•	• •	٠		٠			٠	٠	٠	• •	•		٠	• •		٠	•		٠	٠	• •		٠	• •	٠
•						•							•	• •			•			•		٠		•						•					•			

Where do you go from here?
$\times$ More Algo? $CS 6820$
* More Havdness of Computation? L> Complexity Theory CS 4814
* Both? L> Cryptography CS 4830
Manks for a great semester!