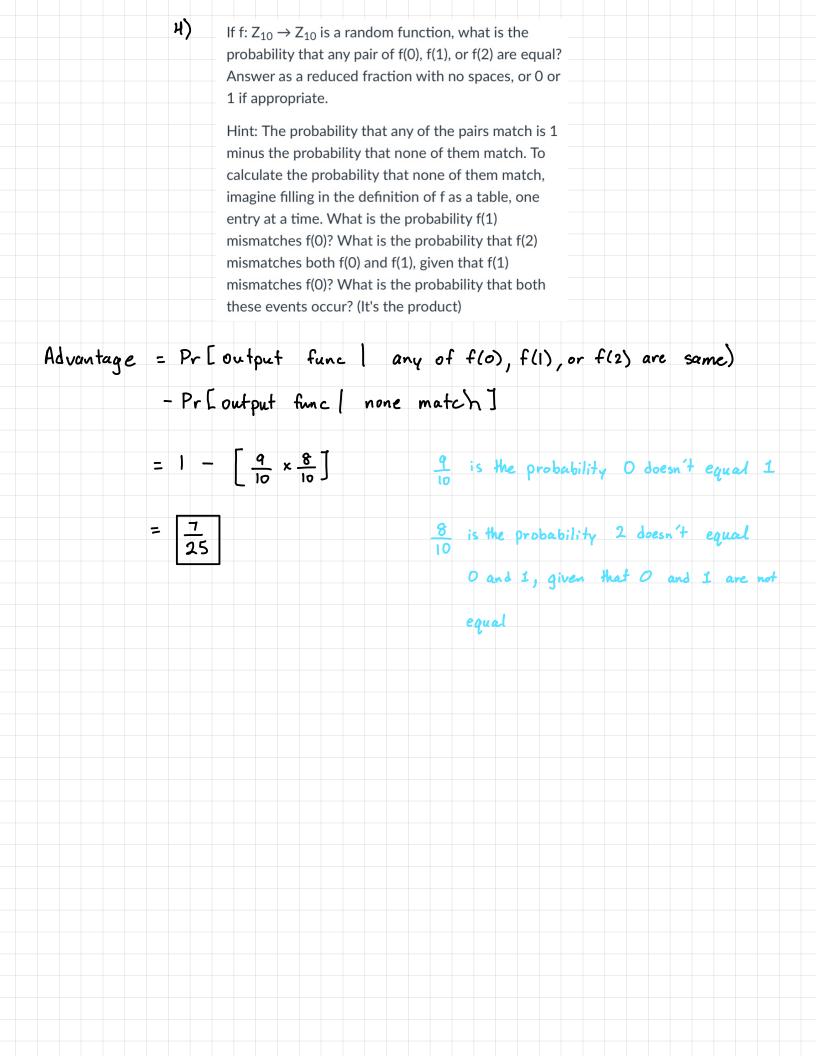
1) You are given a black box f which contains either: (World 1) 3 coins, and with each invocation the 3 coins are all flipped and the number of heads is returned; or (World 2) a 4-sided die, numbered 0-3, and with each invocation the die is rolled and the resulting number is returned. What is the advantage of the following distinguisher? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate. result = f()if (result == 0) output "4-sided die" output "3 coins" Advantage = Pr[output dice | f is dice I - Pr[output dice | f is coins ] Advantage =

	A dvav	ntage	2) = Pr	is not optimadvantage vinvoke fondamental Answer as a 1 if appropri	val. What is the notes when the distingular once.  I reduced fractioniate.	in the previous Question  naximum achievable  uisher is allowed to  n with no spaces, or 0 or  is dice I - Pr Loutput dice I f is coins I
	sult 0	3 c 1 8 3 8	coin	4 side		Since 0 or 3 is more likely to occur we will change the algorith to the following  result = f()
	3 ways	8	ge+ . C3	1 head:	f: I be hea O be tai	
3		s to	- C3		1	# of conditions in if statement # of total outcomes
				Advantage	= 1/2	

3) If f:  $Z_{10} \rightarrow Z_{10}$  is a random permutation, what is the probability that any pair of f(0), f(1), or f(2) are equal? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate. 0 because a permutation doesn't allow duplicate values



5) You are given a black box f which contains either: (World 1) f:  $Z_{10} \rightarrow Z_{10}$  which is a random function; or (World 2) f:  $Z_{10} \rightarrow Z_{10}$  which is a random permutation. What is the advantage of the following distinguisher? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate. if (any of f(0), f(1) or f(2) are the same) output "random function"  $\label{eq:final_sample}$ output "random permutation" Advantage = Pr [ output func | any f are same ] - Pr [ output func | none f are same ] Problem H - Problem 3 0 Advantage =  $\frac{7}{25}$