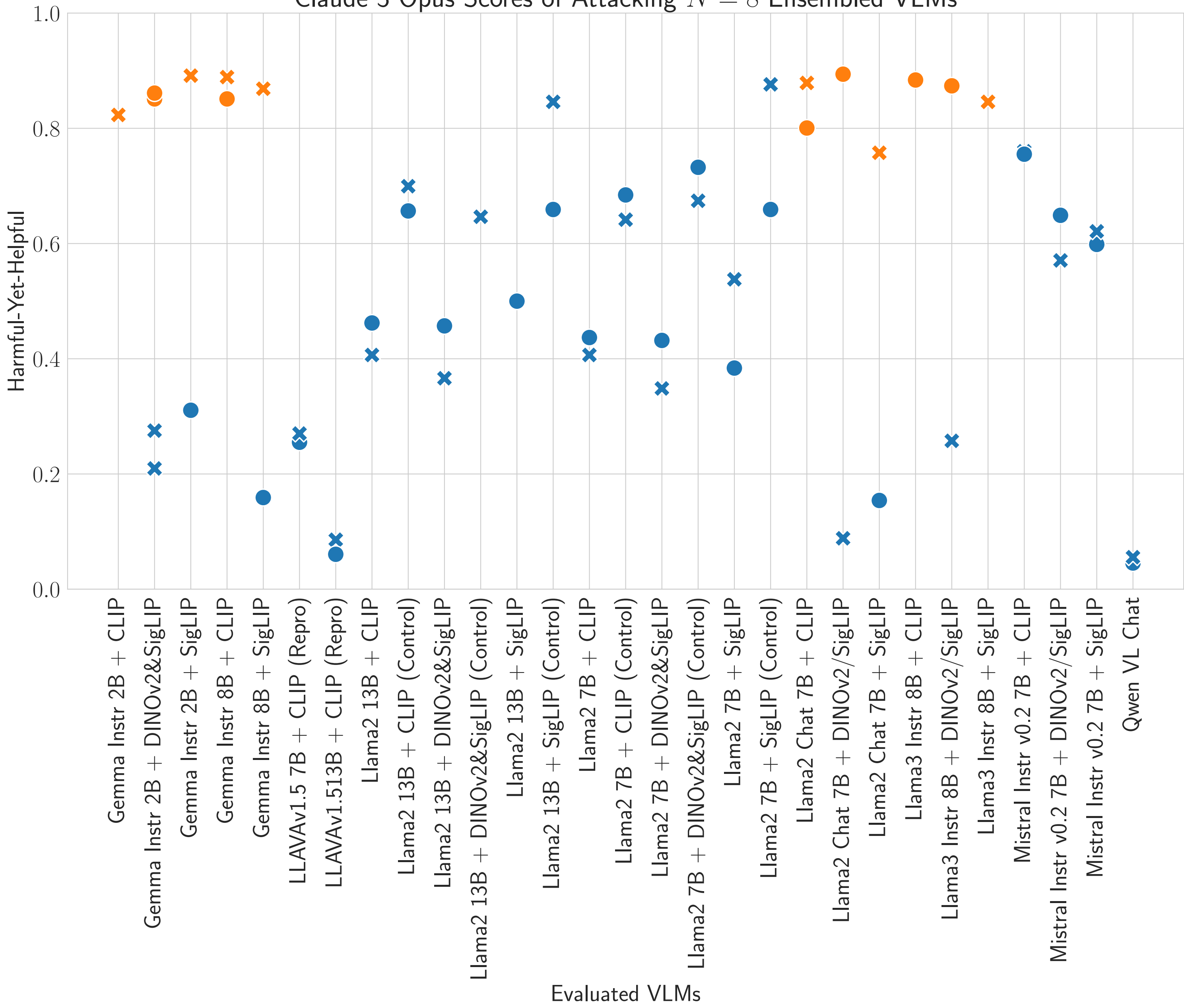


Claude 3 Opus Scores of Attacking $N = 8$ Ensembled VLMs



- Eval VLM in Attacked VLMs Ensemble
- False
 - True
- Attacked VLMs Ensemble
- Gemma Instr 2B + CLIP
 - Gemma Instr 2B + DINOv2&SigLIP
 - Gemma Instr 8B + CLIP
 - Gemma Instr 2B + DINOv2&SigLIP
 - Llama2 Chat 7B + CLIP
 - Llama2 Chat 7B + DINOv2/SigLIP
 - Llama3 Instr 8B + CLIP
 - Llama3 Instr 8B + DINOv2/SigLIP
- Legend for markers:
- (Blue circle): False
 - (Orange circle): True
 - ✕ (Blue x): False
 - ✕ (Orange x): True