Development of a Machine Learning Algorithm for Generating Random Numbers

Wieland, Abraham (School: Aberdeen Central High School)

Individuals, governments, and businesses use cryptography extensively to protect data and prevent theft. Cryptographic security relies heavily on truly random numbers. Various components of cryptography use a random number to make every communication unique. These numbers must be truly random, because even a slight pattern may be reproducible by an attacker. That individual could then gain access to future communications. Because computers are by nature deterministic, it is difficult and time consuming to develop truly random number generators. Thus, a novel solution was approached using machine learning. Neuroevolution of Augmenting Topologies (NEAT) was used with the dieharder suite to develop neural networks capable of generating random numbers. These networks proved competitive against traditional cryptographically secure random number generators on the birthdays test, the only test used in the fitness function in this experiment. This approach proves promising because new algorithms can be developed quickly from existing fitness functions, lowering development costs for new generators.

Awards Won: