2022 부채널정보분석 경진대회

6번 문제 : BNN 가중치 복구

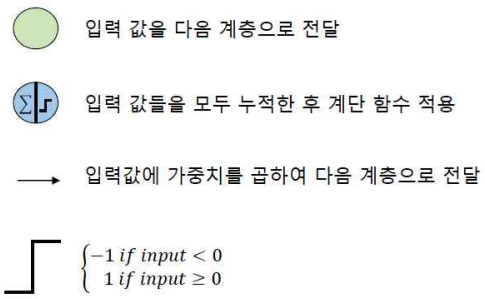
- 문제 요약

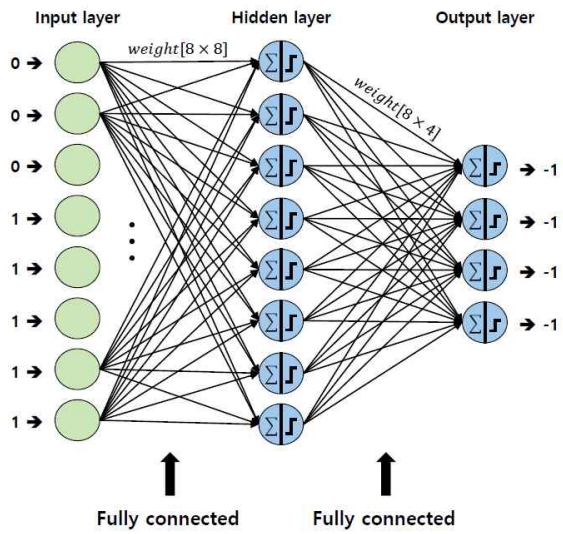
  BNN(Binarized Neural Network)의 모든 가중치를 복구하시오.

- 제공 파일
  - CTF-6-BNN-trace.bin : 주어진 데이터 쌍 추론 과정에서 누출된 BNN의 소비 전력 신호
  - CTF-6-BNN-input.bin : BNN의 입력 (8개의 입력 노드의 값) -> 1byte unsigned integer
  - CTF-6-BNN-output.bin : BNN의 출력 (4개의 출력 노드의 값) -> 1byte **signed** integer

- 참고 사항
  - BNN은 각각 1개의 입력 계층, 은닉 계층, 출력 계층으로 구성됨.
  - 입력 노드 8개, 은닉 노드 8개, 출력 노드 4개로 구성됨.
  - fully-connected BNN 형태임.
  - 모든 가중치는 -1 또는 1의 값을 가짐. (가중치 값은 signed char 형태로 저장)
  - Bias는 존재하지 않음.
  - 입력 노드는 데이터를 입력받아 은닉 계층으로 넘겨줌.
  - 은닉 노드는 입력된 데이터를 누적(sum)하여 계단함수를 적용함.
  - 출력 노드는 입력된 데이터를 누적(sum)하여 계단함수를 적용함.
  - 계단함수는 입력값이 0 미만일 경우 -1을, 0 이상일 경우 1을 출력함.

<Input-output example>
Input: [0, 0, 0, 1, 1, 1, 1, 1]
Output : [-1, -1, 1, -1]





- 플래그
  - 모든 가중치가 복구된 BNN 모델에 아래 32개의 쿼리를 입력.
  - 4개의 출력 노드의 값 중에서 -1을 0으로 치환 후 4비트 이진수로 간주함.
  - 총 32개의 쿼리를 입력하면 4 * 32 = 128비트을 획득할 수 있음.
  - 연접한 128비트를 MSB 부터 차례로 8비트씩 묶은 것이 Flag의 ASCII 코드임.
  - 각 ASCII 코드에 대응하는 문자를 연접하여 플래그 생성.

<플래그 복구를 위한 입력>

[-2, -2, -4, -2, 2, -4, 2, 2]
[0, 5, -1, -1, 1, 3, -2, -1]
[1, -5, 2, -4, 5, 4, -5, -1]
[1, 5, -4, -2, 0, -3, 4, 2]
[4, -3, 4, -3, 4, 1, -3, 5]
[-1, -2, -5, 4, -2, 0, 4, -2]
[-2, -2, -3, -1, 3, -5, 5, 5]
[1, 1, -1, 1, -2, 1, -5, -3]
[2, 0, 0, -5, 3, 3, 2, -3]
[-3, -4, -1, -1, 4, -2, 0, -4]
[-2, -5, 3, -2, 5, -4, -1, 0]
[-4, 0, 0, -3, -2, -5, -3, 5]
[-3, -2, 3, -5, -3, 5, 2, 5]
[5, 0, 2, -3, -2, -4, 0, -3]
[4, -4, -3, -5, -4, -2, 0, 0]
[2, -4, 4, 1, 4, 0, 4, 4]
[5, -5, -5, 1, 3, 5, 3, 2]
[-4, 4, 5, -2, -1, -2, 3, -5]
[1, -4, 1, -2, -1, -5, 4, 4]
[1, 2, 5, -2, 2, -5, -2, 5]
[3, -1, 4, -2, 3, 1, 1, 2]
[5, -4, -2, -5, -2, -5, 5, 0]
[1, 1, -2, -2, 5, 0, 5, 2]
[0, -2, -4, -1, 1, 3, 1, 3]
[4, -5, 5, -4, 0, -4, -1, -2]
[2, -2, -1, -5, 5, 5, 4, -1]
[2, -3, -5, -3, 0, 1, 3, 3]
[5, -4, -1, 0, -2, -1, 0, 1]
[4, -4, -1, -3, 0, 1, 0, 2]
[-3, 0, 5, 0, -5, -2, 3, -2]
[-5, 3, 0, 1, -1, 3, -1, 5]
[-3, -5, -4, -3, 3, -2, -2, -1]

- 참고문헌
  - ref1 : 모델 구조
  - ref2 : Itay Hubara et al., Binarized Neural Networks.