

# NEUROVERKON KÄYTÖN RISKEISTÄ

## Tästä tekstistä

Ohjatulla oppimisella koulutetun neuroverkon toiminta on verkon koulutuksessa käytetyn opetusaineiston tilastollista mallintamista ja mallin soveltamista uuteen aineistoon, jonka oletetaan käyttäytyvän kuten opetusaineisto. Tämä teksti käsittelee seikkoja, jotka neuroverkon käyttäjän tulee ymmärtää tilastolliseen mallintamiseen perustuvista tuloksista, jotta niitä voidaan käyttää oikein ja hallitulla riskillä.

Tekstissä oletetaan lukijan tuntevan neuroverkkojen laskentaperiaatteen ja jonkin verran matematiikkaa. Jos neuroverkot eivät ole lukijalle entuudestaan tuttuja, olisi hyödyksi tutustua aiheeseen ensin vaikkapa perehtymällä kalvosarjaani ”[Mitä tekoäly on ja mitä se ei ole](#)”. Lisäksi voi olla hyödyksi tutustua artikkeliini [Neuroverkko – funktion approksimaattori](#), joka esittelee neuroverkon toimintaa tilastollisena mallintajana. Nämä linkit löytyvät myös tekoälyisivultani, josta löytyy linkkejä myös muuhun tekoälymateriaaliini sekä kaikille avoimien tekoälyesitelmieni ilmoituksiin: <https://www.einouikkanen.fi/AI/>.

Tekstin on kirjoittanut [Eino Uikkanen](#), joka vastaa mieluusti tekstiä koskeviin kysymyksiin osoitteessa [eino.uikkanen@iki.fi](mailto:eino.uikkanen@iki.fi).

## Neuroverkon käytön riskeistä

Ohjatulla oppimisella koulutettu neuroverkko, jäljempänä vain neuroverkko, perustuu opetusaineistoon, josta tunnetaan sekä neuroverkolle syötettävät lähtötiedot että tavoitellut tulostiedot. Neuroverkon kouluttaminen tapahtuu päivittämällä neuroverkon laskenta-parametreja matemaattisesti siten, että neuroverkon opetusaineiston lähtötietojen perusteella antamat tulostiedot poikkeavat mahdollisimman vähän tunnetuista tulostiedoista.

Koulutettu neuroverkko on itse asiassa matemaattisena lausekkeena esitettävissä oleva funktio, joka approksimoi mahdollisimman pienellä virheellä riippuvuutta neuroverkon opetusaineiston lähtötietojen (=funktion argumentit) ja tunnettujen tulostietojen (=funktion arvot) välillä. Neuroverkon koulutusta voidaan siksi kutsua myös tilastolliseksi mallintamiseksi.

Koulutuksen lopputulos on neuroverkon laskentaparametrien päivitettyt arvot. Laskenta-parametrien arvot eivät selitä tarkastelijalle neuroverkon toimintaa, vaikka niiden arvot tunnettaisiin. **Siksi koulutettu neuroverkko on musta laatikko, jonka toimintaa emme pysty selittämään.**

Emme myöskään pysty varmistamaan neuroverkon antamien tulosten oikeellisuutta tai tarkkuutta neuroverkkoon itseensä pohjautuen, vaan ainoastaan ulkoiseen lähteeseen vertaamalla. Tiedämme vain, että **neuroverkko kykenee ennustamaan neuroverkon koulutuksessa käytetyn opetusaineiston tunnetut tulokset keskimäärin tietyllä virheellä.**

Edellä mainitut seikat jättävät neuroverkon tuloksiin alla kuvatut epävarmuustekijät. On huomattava, että kuvatut epävarmuustekijät eivät johdu virheistä tai puutteista neuroverkon tai sitä hyödyntävän sovelluksen rakentamisessa, vaan suoraan neuroverkon toimintavasta eli siitä, että neuroverkko on tilastollista mallintamista ja mallin perusteella tehtyä ennustamista.

*"... neuroverkko kykenee **ennustamaan** koulutuksessa käytetyn opetusaineiston tunnetut tulokset keskimäärin tietyllä virheellä."*

*Neuroverkko on opetusaineiston perusteella rakennettu tilastollinen malli, jonka tulokset ovat mallin perusteella laskettuja ennusteita, eivät täsmällisiä tuloksia. Samasta syystä malli voi antaa tuloksia, jotka eivät ole mielekkäitä lähdeaineistossa.*

*"... neuroverkko kykenee ennustamaan **koulutuksessa käytetyn opetusaineiston tunnetut tulokset keskimäärin tietyllä virheellä."***

*Kun neuroverkkoa sovelletaan opetusaineistoon kuulumattomaan uuteen aineistoon, oletetaan, että uusi aineisto käyttäytyy kuten opetusaineisto. Jos näin ei ole, voi neuroverkon ennustetarkkuus uudella aineistolla olla mielivaltaisen määrän heikompi kuin opetusaineistolla.*

*"... neuroverkko kykenee ennustamaan koulutuksessa käytetyn opetusaineiston tunnetut tulokset **keskimäärin** tietyllä virheellä."*

*Neuroverkon koulutuksessa minimoidaan verkon tulosten keskimääräinen virhe. Yksittäisen tapauksen virheelle tämä ei aseta ylärajaa, ei edes opetusaineistossa.*

Näistä epävarmuustekijöistä johtuen saadaan varmuus neuroverkkojen antamien tulosten oikeellisuudesta tai riittävästä tarkkuudesta vain tarkistamalla ne neuroverkon ulkopuolisesta lähteestä. Tarkistaminen ulkoisesta lähteestä saattaa kuitenkin olla haastavaa tai mahdotonta käytettävissä olevan ajan tai taloudellisten ja muiden resurssien rajallisuuden takia.

Neuroverkon ennustetarkkuutta voidaan toki parantaa esimerkiksi hankkimalla neuroverkon tehtävää paremmin edustavaa tai laajempaa opetusaineistoa, kehittämällä neuroverkon rakennetta tai täsmentämällä ja rajaamalla neuroverkon tehtävää, mutta silloinkin kysymys on vain aste-erosta; neuroverkon antamat tulokset ovat edelleen tilastollisia ennusteita, eivät täsmällisiä tuloksia.

Neuroverkon vastuullisen käyttäjän tulisi siksi arvioida neuroverkon käyttöön liittyviä riskejä ja verrata niitä vaihtoehtoisten ratkaisujen kustannuksiin ja riskeihin.

Hyvin usein vaihtoehtoina ovat kuitenkin vain neuroverkon riskien hyväksyminen sellaisenaan tai luopuminen neuroverkon käyttämisestä kokonaan. Silloin on punnittava, perustelevatko neuroverkon käytöstä saatavat hyödyt sen käytön aiheuttamien riskien hyväksymisen.

Tärkeintä lopulta on kuitenkin ymmärtää, tunnistaa ja tunnustaa yllä esitetyt riskit, jotta niitä osataan joko torjua tai huolelliseen harkintaan perustuen tietoisesti hyväksyä. Kun riskit ymmärretään ja hallitaan, on neuroverkko ennennäkemättömän tehokas ja hyödyllinen työkalu.