Ensamblajes series-paralelo para clasificadores binarios

Idriss Sandoval
idsandov@unirioja.es
Dpto. de Matemáticas y Computación, Universidad de La Rioja

Palabras clave: ensembles, fiabilidad, clasificadores binarios

En este trabajo consideramos ensamblajes (conocidos en inglés como *ensembles*) de clasificadores binarios. Un ensamblaje es una técnica muy conocida y usada en inteligencia artificial que combina las predicciones de varios modelos para generar una predicción final. Dado un conjunto de n clasificadores, existen 2^{2^n} estructuras diferentes para combinarlos. A la hora de diseñar estructuras óptimas para estos ensamblajes usamos conceptos procedentes de la teoría de fiabilidad.

Para reducir el espacio de búsqueda de estructuras eficaces nos restringimos a estructuras series-paralelo, que constituyen un conjunto bien conocido en la teoría de fiabilidad de sistemas.

GENERALIDADES DE FIABILIDAD

La fiabilidad se define como la probabilidad de que un dispositivo realice satisfactoriamente sus funciones previstas durante un período de tiempo específico bajo condiciones de operación específicas. Según esta definición, la fiabilidad se mide como una probabilidad [2]. La teoría de la probabilidad se ha utilizado para analizar la fiabilidad de los componentes, así como la fiabilidad de los sistemas que constan de estos componentes. La fiabilidad se define en términos de un dispositivo, el cual puede ser un componente de un sistema o un sistema que consta de muchos componentes. Dado que el desempeño de un sistema generalmente depende del desempeño de sus componentes, la fiabilidad de un sistema es función de la fiabilidad de sus componentes. En este trabajo se considera los sistemas binarios con componentes también binarios, es decir, aquellos en los que el sistema solo puede estar en dos estados: funcionando o fallando. El estado de un sistema es una

Trabajo financiado por el proyecto INICIA 2023/02 financiado por el Gobierno de La Rioja (España).

función de los estados de sus componentes, es decir, si se conoce el estado de cada componente entonces se puede conocer el estado del sistema.

Supongamos que el sistema tiene n componentes. Si se representa el estado del i-ésimo componente del sistema como una variable binaria x_i, tenemos que para $i = 1, 2, ...n$:

- $x_i = 1$ si el componente i del sistema funciona.
- $x_i = 0$ si el componente i del sistema falla.

El vector de estado de los componentes del sistema viene dado por la n-tupla $X = \{x_1, x_2, ...x_n\}$. Se llama función de estado a la función que permite calcular el estado del sistema a partir del estado de sus componentes y se representa como $\phi = \phi(X)$. De esta manera, tenemos que:

- $\phi(X) = 1$ si el sistema funciona.
- $\phi(X) = 0$ si el sistema ha fallado.

La función de estado del sistema depende de cómo están estructurados sus componentes así como del estado de cada uno. Los sistemas pueden clasificarse en función de su estructura en sistemas serie, sistemas paralelos, sistemas k-de-n y otras estructuras [1].

En la estructura en serie varios componentes están conectados en serie, lo que significa que el sistema fallará si cualquiera de los componentes individuales falla. La fiabilidad total del sistema en serie es el producto de las fiabilidades de cada componente individual. La función de estado del sistema es:

$$\phi(X) = x_1 \times x_2 \times \ldots \times x_n = \min_i \{x_i\} = \prod_{i=1}^{n} x_i$$

donde n es el número de componentes en serie.

En la estructura en paralelo varios componentes están conectados en paralelo, lo que significa que el sistema sigue funcionando mientras al menos uno de los componentes individuales siga funcionando. La fiabilidad total del sistema en paralelo se calcula teniendo en cuenta la probabilidad de que al menos uno de los componentes esté funcionando.

$$\phi(X) = 1 - (1 - x_1) \times (1 - x_2) \times \ldots \times (1 - x_n) = \max_i \{x_i\} = 1 - \prod_{i=1}^{n} (1 - x_i)$$

Un sistema de n componentes iguales tiene una estructura k-de-n si basta que funcionen al menos k cualquiera componentes para que el sistema funcione también. En este caso, la función de estado del sistema es:

$\phi(X) = 1$ si $\sum_{i=1}^{n} x_i \geq k$
y
$\phi(X) = 0$ si $\sum_{i=1}^{n} x_i < k$

MODELOS DE ENSAMBLAJE

Los modelos de ensamblaje en el aprendizaje automático combinan múltiples modelos individuales para mejorar el rendimiento predictivo y la generalización. Hay distintos tipos de modelos de ensamblaje, según cómo se construyan. Los principales son los siguientes:

1. Bagging (Bootstrap Aggregating): Utiliza múltiples conjuntos de datos de entrenamiento, generados mediante el muestreo con reemplazo (bootstrap), para entrenar modelos base. Ejemplos: Random Forest.

2. Boosting: Entrena múltiples modelos secuencialmente, donde cada modelo se enfoca en corregir los errores del modelo anterior. Ejemplos: AdaBoost, Gradient Boosting Machines (GBM), XGBoost, LightGBM, CatBoost.

3. Stacking: Combina las predicciones de múltiples modelos base utilizando otro modelo (a menudo llamado *meta-modelo* o *modelo apilado*) para hacer una predicción final. Puede utilizar un enfoque de entrenamiento de varias etapas.

4. Voting: Puede entenderse como un caso particular del anterior. Combina las predicciones de múltiples modelos base y genera una predicción final mediante algún esquema de votación (por ejemplo, voto mayoritario).

GENERALIDADES EN LA INVESTIGACIÓN

Uno de los principales objetivos del análisis de fiabilidad en procesos industriales es gestionar la redundancia. Los sistemas redundantes suelen ser más fiables, pero la redundancia tiene un coste. El equilibrio entre sistemas fiables y asequibles es un tema principal en el diseño de sistemas basados en la fiabilidad. La propuesta de investigación consiste en aplicar los métodos y principios del diseño de sistemas al diseño y mejora de modelos de ensamblaje en aprendizaje automático. Tomemos como partida los clasificadores binarios que son algoritmos de aprendizaje automático que se utilizan para predecir la pertenencia de un elemento a una de dos clases posibles. Estos algoritmos se basan en la separación de datos en dos categorías distintas, lo que permite tomar decisiones binarias. Se pueden utilizar en una variedad de aplicaciones, como la detección de spam en correos electrónicos, la clasificación de imágenes o la predicción de enfermedades.

Una forma de visualizar los resultados de un modelo de clasificación binaria es mediante la matriz de confusión (ver Cuadro 1.1).

		Predicción	
		Positivo	Negativo
Real	Positivo	Verdadero Positivo (VP)	Falso Negativo (FN)
	Negativo	Falso Positivo (FP)	Verdadero Negativo (VN)

Cuadro 1.1: Matriz de Confusión

Dentro de las métricas de la matriz de confusión encontramos:

$$Precision = \frac{VP}{VP + FP}$$

$$Exactitud = \frac{VP + VN}{VP + FP + FN + VN}$$

$$Sensibilidad = \frac{VP}{VP + FN}$$

$$Especificidad = \frac{VN}{VN + FP}$$

La precisión se encarga de medir la proporción de predicciones correctas sobre el total de predicciones realizadas. La exactitud es la proporción de predicciones correctas sobre el total de observaciones. La sensibilidad o tasa de verdaderos positivos, indica la proporción de casos positivos que fueron correctamente identificados. Por último, la especificidad, o tasa de verdaderos negativos, representa la proporción de casos negativos que fueron correctamente identificados.

Este trabajo pretende asociar conceptos de fiabilidad con métricas de machine learning, de forma que se pueda aplicar técnicas de fiabilidad de sistemas para diseñar estructuras de modelos de ensamblajes. Para ello:

1. Partimos de la fiabilidad ϕ_i de cada modelo del ensamblaje, que se corresponde con la sensibilidad del modelo.

2. Formamos un ensemble mediante una función de estado

3. Podemos estimar de forma sencilla la fiabilidad de cada modelo de ensamblaje a partir de la fiabilidad de cada modelo individual.

De esta manera, probando automáticamente con distintas funciones de estructura y utilizando medidas de importancia como las expuestas en [3], se puede determinar estructuras óptimas para nuestro ensamblaje de modelos de una forma sencilla.

Bibliografía

[1] Solis Alberto. *Fiabilidad, mantenibilidad, efectividad. Un enfoque sistemico.* Universidad Comillas, Madrid, 2000.

[2] Way Kuo and Ming J. Zuo. *Optimal Reliability Modeling.* Wiley and sons, New Jersey, 2003.

[3] Kishor S. Trivedi and Andrea Bobbio. *Reliability and availability engineering.* Cambridge University Press, Cambridge, 2017.