Balance-Subsampled Stable Prediction

Kun Kuang\textsuperscript{1*}, Hengtao Zhang\textsuperscript{2*}, Fei Wu\textsuperscript{1},
Yueting Zhuang\textsuperscript{1}, and Aijun Zhang\textsuperscript{2**}

\textsuperscript{1}College of Computer Science and Technology, Zhejiang University, Hangzhou, China
\textsuperscript{2}Department of Statistics and Actuarial Science, The University of Hong Kong,
Hong Kong, China

Abstract

In machine learning, it is commonly assumed that training and test data share the same population distribution. However, this assumption is often violated in practice because the sample selection bias may induce the distribution shift from training data to test data. Such a model-agnostic distribution shift usually leads to prediction instability across unknown test data. In this paper, we propose a novel balance-subsampled stable prediction (BSSP) algorithm based on the theory of fractional factorial design. It isolates the clear effect of each predictor from the confounding variables. A design-theoretic analysis shows that the proposed method can reduce the confounding effects among predictors induced by the distribution shift, hence improve both the accuracy of parameter estimation and prediction stability. Numerical experiments on both synthetic and real-world data sets demonstrate that our BSSP algorithm significantly outperforms the baseline methods for stable prediction across unknown test data.

Keywords: Stable Prediction; Distribution Shift; Fractional Factorial Design; Subsampling; Regression; Classification.

1 Introduction

One of the most common assumptions in learning algorithms is the homogeneity among training and test samples on which the algorithm is expected to make predictions. However, this condition is often violated in practice due to sample selection bias, which causes distribution shifts between observed data and the population. Moreover, the unknown test distribution leads to an agnostic distribution shift problem. Therefore, it is highly demanding to develop predictive algorithms that are robust to the agnostic distribution shift between training and unknown test data.

In this paper, we assume that the underlying predictive mechanism between predictors/features $X$ and outcome variable $Y$ is invariant across datasets. Based on the invariant predictive mechanism, all predictors $X$ fall into one of two categories. One category includes stable features $S$, which have causal effects on outcome $Y$, and are stable/invariant across datasets. For example in computer

*These authors contributed equally to this work
**Corresponding author: ajzhang@hku.hk
vision, ears, noses, and legs of dogs are stable features to recognize whether an image contains a dog or not. The other category includes noisy features $V$, which have no causal effects on outcome, but might be highly correlated with either stable features, outcome variable or both in certain data sets. For the same example, the grass and background pixels are noisy features for dog recognition. Hence, taking the regression task as an example, we set $X = \{S, V\}$ and have $Y' = f(X) + \epsilon = f(S) + \epsilon$ in our problem. Conditional on the full set of stable features, the noisy features do not affect the expected outcome. However, the distribution shift might make a part of noisy features to become power predictors. In the previous example, grass would be a power predictor if most of the dogs in training data are on the grass. Different distributions shifts might appear in different datasets, leading to the variation of confounding and spurious correlation between the noisy features and outcome variable. To address the stable prediction problem, we should reduce such confounding effects, hence removing the spurious correlations between noisy features and outcome variable.

We assume no prior knowledge about which features are stable and which are noisy. Under such settings, one possible way is to isolate the impact of each individual feature for recovering the true correlation (causation) between predictors and the outcome variable. Variable balancing techniques are widely used for causation recovery in the literature of causal inference. The key idea is to construct sample weights by either employing propensity scores (Rosenbaum and Rubin, 1983, Kuang et al., 2017b, Austin, 2011) or optimizing weights directly (Aihe et al., 2018, Zubizarreta, 2015, Hainmueller, 2012, Kuang et al., 2017a). Recently, a global balancing algorithm (Kuang et al., 2018) was proposed to learn the weights that enforce all features to be as independent as possible, in order to isolate the impact of each feature. Despite its better performance, this algorithm only focuses on the confounding factors between any two variables, while ignoring the higher-order interactions. Moreover, it is not an efficient way by learning the weight for each sample and using full data to perform fitting, especially with huge training samples in big data scenarios.

Full and fractional factorial designs are widely used in statistics for arranging factorial experiments without confounding effects (Box et al., 2005, Dey and Mukerjee, 2009). Using data collected from a factorial designed experiment, one can easily isolate the impact of each feature and reveal the causation between predictors and the outcome variable. Inspired by the factorial designs of experiment, we propose a balance-subsampled stable prediction (BSSP) algorithm, which consists of a factorial design-based subsampling strategy for covariates balancing and a subsampled learning model for stable prediction. Using the factorial design, the subsampling strategy selects a subset of samples from training data such that the covariates are mutually balanced and thus deconfounded. Then, the model fitted by the subsamples would exploit the true correlations between predictors and outcome for stable prediction. Our algorithm has the overwhelming performance across unknown test data with a distribution shift from the training data, thus achieve a more stable prediction. Furthermore, we can train the model faster as the subdata is much smaller than the full data.

In summary, the contributions of this paper are listed as follows:

- We propose a balance-subsampled stable prediction (BSSP) algorithm based on a fractional factorial design-based subsampling strategy for variable deconfounding.

- Theoretically we show that the fractional factorial design-based subsampling can remove the

---

1Here, we call the correlation between noisy features and outcome variable as spurious correlation, since in the generation of the outcome variable, noisy features are supposed to be not correlated with the outcome.
confounding effects with non-linear interactions. Hence, our BSSP algorithm can precisely estimate the parameters and achieve a stable prediction across unknown environments.

- We conduct extensive experiments on both synthetic and real-world datasets, and demonstrate the advantages of our algorithm for stable prediction in both regression and classification tasks.

2 Related Work

Recently, the invariant learning methods have been proposed to explore the invariance across multiple training datasets and used for stable prediction on unknown testing data. Peters et al. (2016) proposed an algorithm to exploit the invariance of a prediction under the causal model, and identify invariant features for causal prediction. Rojas-Carulla et al. (2018) proposed to learn the invariant structure between predictors and the response variable by a causal transfer framework. Similarly, domain generalization methods (Muandet et al., 2013) try to discover an invariant representation of data for prediction on unknown test data. The main drawback of these methods is that their performance highly depends on the diversity of the multiple training data being considered. Moreover, they cannot handle well the distribution shift that does not appear in the existing training data.

Kuang et al. (2018) proposed a global balancing algorithm for stable prediction. As shown in Eq. (2), the global balancing algorithm attempts to learn global sample weights for each sample such that all predictors may become independent. Kuang et al. (2018) also proved that the ideal global sample weights can isolate the impact of each predictor, hence address the stable prediction problem. However, the algorithm in Kuang et al. (2018) is non-convex and only focuses on the first-order confounding between any two variables, ignoring the higher-order interactions.

In statistical designs of experiments, full and fractional factorial designs, especially the two-level factorial designs, are widely used for experimental planning and data collection; see Box et al. (2005), Dey and Mukerjee (2009) and references therein. Resolution and minimum aberration are two main criteria to evaluate the goodness of fractional factorial designs; see Fries and Hunter (1980), Ma and Fang (2001), Xu and Wu (2001), Zhang et al. (2005). These works provide efficient ways of conducting experiments, but not the sample selection methods for observational data.

Subsampling is an efficient strategy to compress the data and accelerate the machine learning algorithm. The idea of sampling is traditionally applied in the survey area and designed to estimate point statistics before observing the response (Thompson, 2012). Recently, it has been leveraged to accelerate the estimation of more complex models. Drineas et al. (2011) and Ma et al. (2015) used the statistical leverages as the probability to resample observations for fitting linear models. Wang et al. (2018) proposed an optimal subsampling based on the A-optimal design for logistic regression, which is further improved by Wang (2019). D-optimal design is adopted in Wang et al. (2019) to select informative subdata for the efficient linear regression. Those methods aim to provide a fast approximation to the model parameters estimated by a given data. What they concern about is the computational efficiency and approximation error on the given training data. Unlike them, this paper considers the idea of subsampling for the stability of model prediction across different and possibly unknown datasets.
3 Problem and Notations

For a prediction problem, we let \( X \) and \( Y \) denote the predictors and outcome variable, respectively. And we define an environment to be the joint distribution \( P_{XY} \) of \( \{X, Y\} \). Let \( E \) denote the set of all environments, and \( M^e = \{X^e, Y^e\} \) be the dataset collected from \( e \in E \). For simplicity, we consider the case where features have finite support. Note that finite support features can be transferred into binary ones via, e.g., dummy encoding. Therefore, without loss of the generality, we assume features \( X \in \{0, 1\}^d \) in this work. In real applications, the joint distribution of features and outcome can vary across environments: \( P^e_{XY} \neq P^e'_{XY} \) for \( e, e' \in E \). The definition of stable prediction (Kuang et al., 2018) is then given as follows:

Problem 1 (Stable Prediction). Given one training environment \( e \in E \) with dataset \( M^e = \{X^e, Y^e\} \), the task is to learn a predictive model that can stably predict across unknown test environments \( E \).

Here, we measure the performance of stable prediction by Average_Error and Stability_Error (Kuang et al., 2018).

\[
\text{Average_Error} = \frac{1}{|E|} \sum_{e \in E} \text{Error}(M^e), \quad \text{Stability_Error} = \sqrt{\frac{1}{|E|-1} \sum_{e \in E} (\text{Error}(M^e) - \text{Average_Error})^2},
\]

where Error\((M^e)\) represents the predictive error on dataset \( M^e \). Now let \( X = \{S, V\} \), where \( S \) denotes stable features and \( V \) denotes noisy features with following assumption (Kuang et al., 2018):

Assumption 1. There exists a probability function \( P(y|s) \) such that for all environment \( e \in E \), \( P(Y^e = y|S^e = s, V^e = v) = P(Y^e = y|S^e = s) = P(y|s) \).

Under assumption 1, one can address the stable prediction problem by developing a predictive model that learns the stable function \( f(S) \) induced by \( P(y|s) \). For example, we have \( f(S) = E(Y|S) = \int yP(y|s)dy \) when \( Y = f(S) + \varepsilon \) with the zero mean error \( \varepsilon \). In practice, we have no prior knowledge on which features belong to \( S \) and which belong to \( V \).

In this paper, we study the stable prediction problem under model misspecification. For simplicity, we only discuss the regression case, and the classification scenario can be similarly derived. Suppose that the true stable function \( f(S) \) and \( Y \) in environment \( e \) are given by:

\[
Y^e = f(S^e) + V^e \beta_V + \varepsilon^e = S^e \beta_S + g(S^e) + V^e \beta_V + \varepsilon^e,
\]

where \( \beta_V = 0 \) and \( \varepsilon^e \perp X^e \). We assume that the analyst mis-specifies the model by omitting non-linear term \( g(S^e) \) and uses a linear model for prediction. Then, standard linear regression may estimate non-zero effects of noisy features \( V^e \) if they are correlated with the omitted term \( g(S^e) \) in the training environment \( e \), which leads to instability on prediction since the following theorem implies that the correlation between \( V \) and \( g(S) \) is changeable across unknown test environments.

Theorem 1. Under assumption 1, the distribution shift across environments is induced by the variation in the joint distribution over \((V, S)\).

Proof.

\[
P(X^e, Y^e) = P(Y^e|X^e)P(X^e) = P(Y^e|S^e, V^e)P(S^e, V^e) = P(Y^e|S^e)P(S^e, V^e)
\]
With assumption 1, we know the distribution $P(Y^e|S^e) = P(Y^{e'}|S^{e'})$ for different $e, e' \in \mathcal{E}$. Hence, the distribution shift across environments (i.e., $P(X^e, Y^e) \neq P(X^{e'}, Y^{e'})$) is induced by the variation in the joint distribution over $(V, S)$ (i.e., $P(S^e, V^e) \neq P(S^{e'}, V^{e'})$).

**Notations.** Let $n$ refer to the sample size, and $d$ be the dimensionality of variables. For any vector $v \in \mathbb{R}^{d \times 1}$, let $\|v\|_1 = \sum_{i=1}^{d} |v_i|$. For any matrix $X \in \mathbb{R}^{n \times d}$, let $X_i,_{j}$ and $X_{i:j}$ represent the $i^{th}$ sample and the $j^{th}$ variable in $X$, respectively. To simplify notations, we remove the environment variable $e$ from $X^e, S^e, V^e, e^e$, and $Y^e$ when there is no confusion from the context.

## 4 Variables Deconfounding

### 4.1 Generalized Global Balancing Loss

Theorem 1 implies that if the covariates are mutually independent (or there are no confounding effects among variables), we can well estimate parameter $\beta_V$ in Eq. (1), hence improve the stability of prediction across unknown test environments. The confounding effects between covariates and the binary treatment status are typically eliminated by balancing covariates in causality literature (Athey et al., 2018; Austin, 2011; Hainmueller, 2012). Recently, Kuang et al. (2018) successively regarded each variable as the treatment indicator and minimized a global balancing loss:

$$
\min_{W \in \mathbb{R}^n} \mathcal{L}(W, X) = \frac{d}{\sum_{j=1}^{d} \left( \frac{X^T_{i:j} (W \odot X_{-j})}{W \cdot X_{-j}} - \frac{X^T_{i:j} (W \odot (1 - X_{-j}))}{W \cdot (1 - X_{-j})} \right)^2}
$$

where $\odot$ refers to Hadamard product; $X_{-j} = X \setminus \{X_{-j}\}$ means all the remaining variables by removing the $j^{th}$ variable in $X$; and $X_{i:j}$ denotes the $(i, j)$ entry in $X$. The difference in quadratic loss enforces $P_W(X_k = 1|X_j = 1) \approx P_W(X_k = 1|X_j = 0)$ w.r.t. the weighted conditional distribution $P_W$. When the equation holds exactly, it can be shown that $X_k \in \{0, 1\}$ and $X_j \in \{0, 1\}$ are independent and thus have no confounding effects. $\mathcal{L}(W, X)$ hence globally balances each variable with others by reweighting the observations. Despite effectiveness, Eq. (2) can only remove the first-order confounding effect among variables, while ignoring the higher-order ones, for example, between $V$ and a $k$-way interaction function $g(S)$. Moreover, it is not a convex optimization problem and the global optima is hard to find. Finally, using full weighted data can be computationally expensive for further training especially in the big data scenarios.

Considering high-order confounding effects among variables, we define a new generalized global balancing loss $\mathcal{L}_k(W, X)$ as:

$$
\mathcal{L}_k(W, X) = \sum_{j \in [d]} \sum_{I_k \subseteq [d] \setminus \{j\}} \left[ \frac{X^T_{i:j} (W \odot X_{-j})}{W \cdot X_{-j}} - \frac{X^T_{i:j} (W \odot (1 - X_{-j}))}{W \cdot (1 - X_{-j})} \right]^2
$$

where $k$ refers to the order of confounding effect with $1 \leq k < d$, and $X_{i:j}, X_{i:k}$ denote the $k$-way interaction w.r.t. the index subset $I_k$. This loss broadly measures different orders of correlation or
confounding effect between V and g(S). It is easy to see that Eq. (2) is a special case of Eq. (3) with \( k = 1 \). Our target in this paper is to minimize the aggregation of \( L_k(W, X) \) up to the order \( k \).

4.2 Variables Deconfounding via FFDs

In this section, we elaborate on how FFDs can be used to deconfound the variables in terms of minimizing the generalized balancing loss in Eq. (3). Note that the binary-encoded data matrix is closely related to a two-level factorial design, which motivates us to leverage the classical results from the fractional factorial design literature.

Two-level fractional factorial design (FFD) (Dey and Mukerjee, 2009): It is a size-\( m \) subset of the full factorial design that consists of all \( 2^d \) possible combinations of the vector \( \{-1, 1\}^d \). We denote FFD by \( D \in \{-1, 1\}^{m \times d} \), where \( 0 < m < 2^d \).

One important feature of FFD is that variables and their interactions are orthogonal to some degrees, and they can achieve joint orthogonality when FFD becomes full factorial. Another cardinal observation is that the mean differences in Eq. (3) can be transferred into the inner products of the main effects and high-order interactions of a design in \( \{-1, 1\}^{m \times d} \); see the proof of Theorem 3. Consequently, the orthogonality of FFD can help remove non-zero inner products and lead to a minimal loss.

Resolution (Fries and Hunter, 1980), denoted as \( R \), is an important criterion to reflect the degree of orthogonality. For an FFD, define the generalized word-length pattern (Ma and Fang, 2001)

\[
W(D) = (A_1(D), \ldots, A_d(D)),
\]

where \( A_j(D) \) refers to the generalized wordlength and measures the degree of \( j \)-factor non-orthogonality. Specifically,

\[
A_j(D) = \frac{1}{m(q-1)} \sum_{k=0}^{d} P_j(k; d, q) B_j(D), \quad j = 1, \ldots, d,
\]

(4)

where \( q \) denotes the number of levels,

\[
P_j(x; d, q) = \sum_{w=0}^{j} (-1)^w (q - 1)^{j-w} \binom{d-x}{j-w}
\]

are the Krawtchouk polynomials (MacWilliams and Sloane, 1977), and \( B(D) = (B_0(D), \ldots, B_d(D)) \) is the distance distribution \( B_j(D) = m^{-1} \left| \{ (c, d) : d_H(c, d) = j, c, d \in D \} \right| \) with \( d_H(\cdot, \cdot) \) denoting the Hamming distance. Note that \( B_j(D) \) is invariant to the encoding way of \( D \). Then, the resolution of \( D \) is defined as the smallest index \( R \leq d \) such that \( A_R(D) > 0 \). Note that the full factorial design with \( m = 2^d \) has resolution \( d + 1 \), since \( A_j(D) = 0 \) for all \( j \in [d] \).

The following lemma (Hedayat et al., 2012) explains the relationship between resolution \( R \) and orthogonal strength. We omit ‘fractional factorial’ in the resolution-\( R \) design without ambiguity to the context.

Lemma 1. The resolution-\( R \) design \( D \) has orthogonal strength \( t = R - 1 \), where \( t \) means that one can see all possible \( t \)-tuples equally often for \( m/2^t \) times in any \( t \) columns of \( D \).

Lemma 1 implies that any \( t \) columns/variables of \( D \) contain \( m/2^t \) full factorials such that every \( t \) factors are jointly orthogonal. Furthermore, this lemma also implies low order \( t' < t \) orthogonal strength exists for the resolution-\( R \) design. In other words, FFD can preserve the joint
orthogonality up to its resolution minus one. For example, a resolution-3 design guarantees the pairwise orthogonality among the main effects of all factors. The following theorem further states the preserved orthogonality among the main effect and their \( k \)-way interaction.

**Theorem 2.** Let \( I_k \subseteq [d] \) denote any collection of distinctive factors with \(|I_k| = k \leq d\), \( D = (D_1, \ldots, D_d) \in \{-1, 1\}^{m \times d} \) be the design matrix, and \( D_{I_k} \in \{-1, 1\}^m \) represent \( k \)-way interaction of \( I_k \). We have a) \( D_{I_k}^T D_{I_j} = 0, i \neq j \), for any resolution-\( R \) design with \( R \geq 3 \); and b) \( D_{I_k}^T D_{I_j} = 0, j \in [d], 2 \leq k \leq R - 2 \), for any resolution-\( R \) design with \( R \geq 4 \).

**Proof.** To prove above theorem, we first inductively show a lemma that any full factorial design (FD) denoted by \( D \in \{-1, 1\}^{2^d \times d} \) has \( 1^T D_{I_d} = 0 \) for the integer \( d \geq 1 \). It is easy to check that \( 1^T D_{I_d} = 0 \) holds when \( d = 1, 2 \). Suppose this equality holds for any integer \( d = \ell, \ell \geq 1 \). When \( d = \ell + 1 \), note that \( D \) is invariant to the permutation of rows, so we rearrange the first column and have

\[
D_{I_{d+1}} = \left( -1, \ldots, -1, 1, \ldots, 1 \right)^T \odot (D_{I_\ell}^{(1)}, D_{I_\ell}^{(2)})^T,
\]

where the sub-designs \( D^{(1)}, D^{(2)} \subseteq \{-1, 1\}^{2^\ell \times \ell} \) also belong to FD (Hedayat et al., 2012). Therefore, it can be derived that \( 1^T D_{I_{d+1}} = 1^T D_{I_\ell}^{(2)} - 1^T D_{I_\ell}^{(1)} = 0 \) and the statement gets proved. So for any FFD with orthogonal strength \( t \), we have \( 1^T D_{I_k} = 0 \) for \( k \in [t] \), because Lemma 1 tells that all combinations of at most \( t \)-tuples (full factorial design) appear with equal frequency in corresponding distinctive columns.

With the above property, we can easily show the first case in the theorem as \( D_{I_d}^T D_{I_d} = 1^T D_{I_2} \) with \( I_2 = \{i, j\} \), and the resolution-\( R \) design has orthogonal strength \( t = R - 1 \geq 2 \), which implies \( D_{I_2}^T D_{I_2} = 0 \). For the second case, we restate it in terms of orthogonal strength \( t \), that is, we need to show \( D_{I_k}^T D_{I_j} = 0, j \in [d], 2 \leq k \leq t - 1 \) for \( t \geq 3 \), which can be inductively proved in the similar manner. Without loss of the generality, we just show \( D_{I_k}^T D_{I_j} = 0 \) for \( t = 3 \) in what follows. When \( j \notin I_2 \), we can construct a 3-column FFD with indices \( I_3 = \{j\} \cup I_2 \) and \( D_{I_3}^T D_{I_3} = 1^T D_{I_3} \). And we can similarly obtain \( 1^T D_{I_3} = 0 \) as done in the first case because of \( t = 3 \). If \( j \in I_2 = \{i, j\} \), it is easy to check that \( D_{I_2}^T D_{I_2} = 1^T D_{I_2} = 0 \) as \( t = 3 \). For \( t \geq 4 \), since high-order orthogonal strength implies the low order ones, we only need to consider the situation of \( k = t - 1 \). And we can similarly obtain the conclusion by discussing \( j \) in \( I_k \) or not.

With these results of FFD, if we determine the subdata matrix \( X \in \{0, 1\}^{m \times d} \) by exactly matching it to some resolution-\( R \) design \( D \in \{-1, 1\}^{m \times d} \) with the rule \( D_{I_j} = 2X_{I_j} - 1 \). We can show that such \( X \) is the optimal solution of Eq. (3) with weights \( W = 1 \).

**Theorem 3.** For any \( X \in \{0, 1\}^{m \times d} \) matching the resolution-\( R \) design with \( R \geq 3 \), we have \( \mathcal{L}_k(W, X) = 0 \) for any \( 1 \leq k \leq R - 2 \) and \( W = 1 \).

**Proof.** Let \( D \in \{-1, 1\}^{m \times d} \) be the resolution-\( R \) design matched with \( X \). For any \( I_k \subseteq [d] \setminus \{j\} \) with a given \( j \) and feasible \( k \), let \( I_k = \{j_1, \ldots, j_k\} \) and we have

\[
X_{I_k} = \frac{1}{2^k} (D_{j_1} + 1) \odot \cdots \odot (D_{j_k} + 1) = \frac{1}{2^k} \left( 1 + \sum_{h=1}^k \sum_{I_h \subseteq I_k} D_{I_h} \right),
\]
where $\tilde{I}_h$ is the subset of $I_k$ with cardinality $h$. When $W = 1$, we have

$$
\left[ \frac{X^T_{I_h} (W \odot X_{-j})}{W^T X_{-j}} - \frac{X^T_{I_h} (W \odot (1 - X_{-j}))}{W^T (1 - X_{-j})} \right]^2 \\
\left[ \frac{2}{m} X^T_{I_k} (2X_{-j} - 1) \right]^2 = \left( \frac{2}{m} X^T_{I_k} D_{-j} \right)^2 \\
= \frac{1}{4^{k-1}} \left( \sum_{h=1}^{k} \sum_{I_h \subseteq I_k} D^T_{I_h} D_{-j} \right)^2 = 0,
$$

where the last equality follows Theorem 2. Specifically, when $k = 1$ or $R = 3$, we have $\tilde{I}_h = I_k = \{j_k\}$ with $j_k \neq j$ and the last equality becomes zero according to the case a) in Theorem 2. Similar results can be derived for $2 \leq k \leq R - 2$ ($R \geq 4$) following the case b). Consequently, it is evident that $L_k(1, X)$ equals to zero for any $1 \leq k \leq R - 2$ ($R \geq 3$).

This theorem reveals that higher resolution design can lead to more stable outcomes, as the lower-order confounding effects are removed by the perfect balance. Since a higher resolution design would require a larger run size $m$. In the present paper, we use resolution-5 design as a subsampling template, which ensures $L_k(1, X) = 0$ for $k = 1, 2, 3$. The template can be easily generated from open source packages, such as FrF2 in R [Grömping 2014]. Finally, we can significantly save the calculation time for model training based on selected data, as $m$ is typically much smaller than full data size $n$.

We end this section with a toy example in Fig. 1 which illustrates the main idea of different deconfounding methods. Consider a three-dimensional data set with binary input. We visualize the sample space in Fig. 1a and the bubble size corresponds to the number of observations on that point. Note that each facet corresponds to the conditional distribution of two variables w.r.t. the remaining one. Therefore, all bubbles should have the same size in the ideal case when there are no confounding effects among variables, since any two opposite facets should have the same distribution. To achieve this goal, global balancing method (Fig. 1b) takes all sample values but reweights them to change the data distribution. It is easy to see that the ideal case accords with the full factorial design where all possible sample values appear with the same frequencies. So our subsampling method (Fig. 1c) only uses a fraction of samples that well represent the ideal situation. For example, the conditional distributions of $X_i|X_k$ and $X_j|X_k$ are the same in Fig. 1c where $i, j, k \in \{1, 2, 3\}$ are distinctive indices.

Figure 1: A toy example to illustrate the main idea of each deconfounding method.
5 BSSP Algorithm

BSSP algorithm consists of an FFD-based subsampling method and a subsampled learning model. We first introduce the specific subsampling algorithm that is feasible for general situations. To obtain a balanced subdata with deconfounded variables, we propose a matching algorithm based on the FFD template. Given a resolution-$R$ design $D \in \{-1, 1\}^{m \times d}$, let $M = \{X \in \{0, 1\}^{n \times d}, Y \in \mathbb{R}^n\}$ if some row in $D$ can match the one in $X$. The matching processes are described in Algorithm 1.

Algorithm 1 Sample_Matching Algorithm

Require: Observed samples $M = \{X \in \{0, 1\}^{n \times d}, Y \in \mathbb{R}^n\}$ and a design $D \in \{0, 1\}^{m \times d}$
Ensure: A subset of samples $M_{\text{sub}}$

1: Set $M_{\text{sub}} = \emptyset$
2: for each row/sample $D_i, i \in D$ do
3:   if $D_i = X_j, j$ then
4:      $M_{\text{sub}} = M_{\text{sub}} \cup (X_j, Y_j)$
5:      break
6: end if
7: end for
8: return $M_{\text{sub}}$

However, it may not be easy to achieve a perfect matching and thus non-confounding properties in practice. Note that Lemma 1 implies the orthogonality is invariant to the column permutation of $D$, which we may denote as $D$ with the cardinality $d!$. All the designs in $D$ share the same orthogonal properties as the template design $D$. Hence, we may find a better design $D'$ in $D$ such that all its design points can be matched to the observed samples.

If none of the designs in $D$ can be fully matched to the observed samples in $X$, we propose a confounding measure to evaluate the degree of confounding properties for $M_{\text{sub}} = \{\tilde{X}, \tilde{Y}\}$:

$$\psi(M_{\text{sub}}) = \sum_{j=1}^{R-1} \rho^j A_j(\tilde{X}), \quad 0 < \rho < 1, \quad (5)$$

where $A_j(\tilde{X})$ refers to the generalized wordlength in Eq. (4) and $\rho$ is a parameter for exponentially weighing. In the ideal case, we have $\psi(M_{\text{sub}}) = 0$ according to the definition of resolution-$R$ design. Note that $A_j(\tilde{X})$ reflects the severity of order-$j$ confounding effects and is invariant to the design encoding. Motivated by the famous effect hierarchy principle [Wu and Hamada (2011): (i) lower-order effects are more likely to be important; and (ii) effects with the same order are equally likely to be important, we set $\rho = 0.9$ to assign more weights to the lower-order effects.

A simulation is performed shown by Fig. 2 to validate that $\psi(M_{\text{sub}})$ can measure the deviation of $\tilde{X}$ to the FFD, where we calculate the $\psi(M_{\text{sub}})$ on random subsets of a 128-run resolution-5 design with different sizes and 100 replications. As we can see, the measure goes to 0 without any variation when $\tilde{X}$ is close to the template design.

Based on Eq. (5), one can calculate the confounding measure for each $D$ in $D$. Then, we can rank these subdata candidates and select the one with the minimal $\psi$-value. The details of the complete subsampling method are described in Algorithm 2.
Algorithm 2 FFD-Based Subsampling Algorithm

Require: Observed samples $M = \{X \in \{0, 1\}^{n \times d}, Y \in \mathbb{R}^{n}\}$ and a resolution-$R$ design $D \in \{0, 1\}^{m \times d}$.

Ensure: A subset of samples $M_{\text{sub}}$

1: Set $M_{\text{sub}} = \emptyset$
2: Generate a design set $D$ by column permutation on $D$,
3: for $D' \in D$ do
4: $M'_{\text{sub}} = \text{Sample\_Matching} (M, D')$
5: Calculate its confounding measure $\psi(M'_{\text{sub}})$
6: if $\psi(M'_{\text{sub}}) < \psi(M_{\text{sub}})$ then
7: Let $M_{\text{sub}} = M'_{\text{sub}}$
8: end if
9: if $\psi(M_{\text{sub}}) == 0$ then ▷ all samples in $D'$ are matched
10: break
11: end if
12: end for
13: return $M_{\text{sub}}$

With the balance-subsampled data $M_{\text{sub}}$ from Algorithm 2, one can directly run a machine learning model for prediction, including regression for continuous outcome $Y$ and classification for categorized outcome $Y$. In this work, we simply consider the typical linear regression and logistic model with the original linear features of $\tilde{X}$.

6 Experiments

We compare our BSSP with three algorithms in the experiments. Traditional Logistic Regression (LR) and Ordinary Least Square (OLS) are set to be the baseline methods for classification and regression tasks, respectively. As for the benchmark of stable learning, we consider the Global Balancing Regression (GBR) [Kuang et al., 2018]. It learns the global weights for all samples in order to make the variables approximately non-confounding, and then performs weighted classification and regression by LR and OLS. Additionally, the LASSO regularizer [Tibshirani, 1996] is configured in all methods. The performance of different approaches are then evaluated by RMSE of predicted outcomes, $\beta$\_Error ($\|\beta - \hat{\beta}\|_1$), Average\_Error, and Stability\_Error, where we define Error($M^c$) = RMSE($M^c$) in Average\_Error and Stability\_Error. A resolution-5 design with $m = 128$ is used as the template for experiments.

6.1 Synthetic Datasets

6.1.1 Stable Prediction for Regression Task

Datasets. We generate binary predictors $X = \{S_{1,1}, \ldots, S_{1,5}, V_{1,1}, \ldots, V_{1,5}\}$ with independent entries from $\mathcal{N}(0, 1)$. Then we binarize the variable by setting $X_{1,j} = 1$ if $X_{1,j} \geq 0$, otherwise $X_{1,j} = 0$. Finally, we generate continuous response variable $Y$ following Eq. (1), where $\beta_{S} = \ldots$
we report Average_Error and Stability_Error to evaluate the stability of prediction (See Fig. 3d).

Figure 2: $\psi(M_{\text{sub}})$ on random subsets of a 128-run resolution-5 FFD with different subdata sizes.

Figure 3: Results of regression. All the models are trained with $n = 2000$, $d = 10$ and $r_{\text{train}} = 2.0$.

$[\frac{1}{3}, -\frac{2}{3}, 1, -\frac{1}{3}, \frac{2}{3}]$, $\beta_V = 0$, and $\varepsilon \sim \mathcal{N}(0, 0.3^2)$. The non-linear term $g(\cdot)$ is set to be $S_{i,1}S_{i,2}$. To test the stability of the algorithm, we vary the environment via a biased sample selection with a rate of $r \in [-3, -1] \cup (1, 3]$. Specifically, we select the sample with a probability $p = |r|^{-5\tau}$, where $\tau = |S\beta_S + S_{i,1}S_{i,2} - \text{sign}(r)V_5|$. The sign of $r$ determines the type of correlation between $Y$ and $V_5$. $r > 0$ refers to a positive correlation and $|r|$ quantifies the magnitude of correlation. We generate $n = 2000$ samples after the biased selection.

**Results.** We train all models in the same environment with $r_{\text{train}} = 2$, and replicate the training for 50 times. We report mean and variance of $\beta_{\text{Error}}$ under the training environment in Fig. 3a & 3b. To evaluate the stability of prediction, we test all models on various test environments with different bias rates $r_{\text{test}} \in \{-3, -2, -1.7, -1.5, -1.3, 1.3, 1.5, 1.7, 2, 3\}$. For each $r_{\text{test}}$, we generate 50 independent test datasets and report the averaged RMSE in Fig. 3c. Given RMSEs, we report Average_Error and Stability_Error to evaluate the stability of prediction (See Fig. 3d). Compared with baselines, the BSSP algorithm achieves a more precise estimation of the parameters and the best stable prediction across unknown test environments with fewer samples.

### 6.1.2 Stable Prediction for Classification Task

**Datasets.** The covariates are simulated from the same process in the regression task. But we generate binary response variable $Y$ from the function as follows:

$$Y = \frac{1}{1 + \exp(-\sum_{i=1}^{3} \alpha_i \cdot S_{.,i} - 5 \cdot S_{.,4} \cdot S_{.,5})) + \mathcal{N}(0, 0.2^2).$$
On the weighted data from GBR
On subsampled data from BSSP

Figure 4: Results of classification on various test datasets by varying \( r_{\text{train}} \).

(a) \( r_{\text{train}} = 0.15 \)  
(b) \( r_{\text{train}} = 0.25 \)  
(c) \( r_{\text{train}} = 0.75 \)  
(d) \( r_{\text{train}} = 0.85 \)

Figure 5: Pearson correlation coefficients among variables: a) on raw data; b) on weighted data from global balancing; c) on subsampled data from BSSP.

We define \( \alpha_i = (-1)^i \cdot (\text{mod}(i, 3) + 1) \cdot d/3 \), where function \( \text{mod}(x, y) \) returns the modulus after the division of \( x \) by \( y \). To make \( Y \) binary, we set \( Y = 1 \) when \( Y \geq 0.5 \), otherwise \( Y = 0 \). Furthermore, different environments are generated by varying \( P(Y|V_5) \) with a biased sampling rate \( r \in (0, 1) \). Specifically, we select a sample with probability \( r \) if \( V_5 = Y \); otherwise, we select it with probability \( 1 - r \), where \( r > 0.5 \) corresponds to a positive correlation between \( Y \) and \( V \). And larger \( r \) leads to stronger correlation. \( n = 2000 \) samples are generated after selection.

Results. In our experiments, we generate different synthetic data by varying bias rate \( r_{\text{train}} \in \{0.15, 0.25, 0.75, 0.85\} \). For each \( r_{\text{train}} \), we set \( r_{\text{test}} \in \{0.1, 0.2, \ldots, 1\} \). The averaged RMSE of 50 replications on each training data is visualized in Fig. 4. As we can see, the suspicious correlation between \( V_5 \) and \( Y \) can improve the performance of baselines when \( r_{\text{train}} \approx r_{\text{test}} \), but it causes instability of prediction to LR or GBR when the training and test environments are quite different. Compared with baselines, the RMSE of our BSSP algorithm is consistently stable and small across different environments. Moreover, BSSP makes greater improvements when \( r \) is farther from 0.5.

6.1.3 Pearson Correlation Coefficients

Under the synthetic regression setting, we compare the Pearson correlation coefficients between any two variables of various approaches in Fig. 5. This experiment demonstrates how different methods remove the confounding effects among variables.

From the result, we can find that in the raw data (Fig. 5a), the noisy feature \( V_5 \) is correlated with some stable features \( S \), the nonlinear term \( g \) and outcome \( Y \). Hence, the estimated coefficient of \( V_5 \) in OLS would be large and thus leads to unstable prediction. In the weighted data by GBR (Fig. 5b), the sample weights learned from global balancing can clearly remove the correlation between noisy feature \( V_5 \) and stable features \( S \). But \( V_5 \) is still correlated with both omitted nonlinear term \( g \) and outcome \( Y \), leading to imprecise estimation on \( \beta_Y \) and unstable prediction. The main reason is
that the global balancing method only considers first-order confounding effects while ignoring the higher-order effect between $V_5$ and $g$. In BSSP (Fig. 5c), we can find that not only the correlation among predictors $X$, but also the one between $V_5$ and $g$ as well as $Y$ is clearly removed. Hence, our BSSP algorithm can estimate the coefficient of both $S$ and $V$ more precisely. This is the key reason that BSSP can make more stable predictions across unknown test environments.

### 6.2 Real Datasets

To check the performance of the BSSP algorithm on the real-world data. We apply it to a WeChat advertising dataset (classification) and Parkinson’s telemonitoring data (regression), respectively. The detailed descriptions of datasets and preprocessing are listed in what follows.

**WeChat Advertising Dataset.** It is a real online advertising dataset, which is collected from Tencent WeChat App\(^2\) during September 2015 and used in [Kuang et al., 2018] for stable prediction. In WeChat, each user can share (receive) posts to (from) his/her friends like Twitter and Facebook. Then the advertisers could push their advertisements to users, by merging them into the list of the user’s wall posts. For each advertisement, there are two types of feedbacks: “Like” and “Dislike”. When the user clicks the “Like” button, his/her friends will receive the advertisements.

The WeChat advertising campaign used in our paper is about the LONGCHAMP handbags for young women\(^3\). This campaign contains 14,891 user feedbacks with Like and 93,108 Dislikes. For each user, we have their features including (1) demographic attributes, such as age, gender, (2) number of friends, (3) device (iOS or Android), and (4) the user settings on WeChat, for example, whether allowing strangers to see his/her album and whether installing the online payment service.

In our experiments, we set $Y_i = 1$ if user $i$ likes the ad, otherwise $Y_i = 0$. For non-binary features, we dichotomize them around their mean value. And we only preserve users’ features which satisfied $0.2 \leq \frac{\# \{x=1\}}{\# \{x=1\} + \# \{x=0\}} \leq 0.8$. Finally, our dataset contains 10 binary user features as predictors and user feedback as the outcome variable. To test the stability of all methods, we separate the whole dataset into 4 parts by users’ age, including Age $\in [20, 30)$, Age $\in [30, 40)$, Age $\in [40, 50)$ and Age $\in [50, 100)$. All models are trained with data from the environment Age $\in [20, 30)$ but are tested on all 4 environments.

**Parkinson’s Telemonitoring Dataset.** To test BSSP in a regression setting, we apply it to a Parkinson’s telemonitoring dataset\(^4\) which has been wildly used for domain generalization [Muandet et al., 2013, Blanchard et al., 2017] task and other regression task [Tsanas et al., 2009]. The dataset is composed of biomedical voice measurements from 42 patients with early-stage Parkinson’s disease. For each patient, there are around 200 recordings, which were automatically captured in the patients’ homes. The aim is to predict the clinician’s motor and total UPDRS scores of Parkinson’s disease symptoms from patients’ features, including their age, gender, test time and many other measures.

In our experiments, we alternately set the outcome variables $Y$ as motor UPDRS scores and total UPDRS scores. For those non-binary features, we dichotomize them around their mean value. Finally, we selected 10 patients features as predictors $X$, including age, gender, test time, age, gender, test time, age, gender, test time.

---

1. http://www.wechat.com/en/
2. http://en.longchamp.com/en/womens-bags
3. https://archive.ics.uci.edu/ml/datasets/parkinsons+telemonitoring
Figure 6: Prediction across environments of each method in different datasets. The models are all trained on the first environment, but tested across different groups.

Jitter: PPQ5 (a measure of variation in fundamental frequency), Shimmer: APQ5 (a measure of variation in amplitude), RPDE (a nonlinear dynamical complexity measure), DFA (signal fractal scaling exponent), PPE (a nonlinear measure of fundamental frequency variation), NHR and HNR (two measures of the ratio of noise to tonal components in the voice).

To test the stability of all algorithms, we separate the whole 42 patients into 4 patients’ groups, including PG1 with recordings from 21 patients, and the other three groups (PG2, PG3, and PG4) are all with recordings from different 7 patients. We train models with data from environment PG1, but test them on all 4 environments.

**Results.** We visualize the results in Figure 6. From the figure, we can obtain that the proposed BSSP algorithm achieves comparable results to the baseline OLS/LR on training environment. On the other three test environments, whose distributions differ from the training environment, BSSP achieves the best prediction performance. Another important observation is that the performance of our algorithm is always better than the global balancing method. The main reason is that GBR, unlike our BSSP algorithm, cannot address the high-order confounding among variables.

### 7 Conclusion

This paper addresses the problem of stable prediction across unknown environments. We propose a subsampling method to reduce the spurious correlation between noisy features and the outcome variable. The subsampling method uses fractional factorial design as a matching template, which can promote the non-confounding properties among predictors if one can find a subdata to fully match the design. We also propose a new confounding measure to guide the subsample selection in general situations. Our method can be regarded as a data pre-treatment so that it can be applied to different prediction tasks, such as regression and classification. Extensive experiments on both synthetic and real-world datasets have clearly demonstrated the advantages of our proposed method for stable prediction. Our future work will focus on the subsampling based on $k$-level fractional factorial designs and space-filling designs, aiming to address the stable prediction problem with multi-level and continuous variables.
References

Susan Athey, Guido W Imbens, and Stefan Wager. Approximate residual balancing: debiased inference of average treatment effects in high dimensions. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 80(4):597–623, 2018.

Peter C Austin. An introduction to propensity score methods for reducing the effects of confounding in observational studies. *Multivariate Behavioral Research*, 46(3):399–424, 2011.

Gilles Blanchard, Aniket Anand Deshmukh, Urun Dogan, Gyemin Lee, and Clayton Scott. Domain generalization by marginal transfer learning. *arXiv preprint arXiv:1711.07910*, 2017.

George EP Box, J Stuart Hunter, and William G Hunter. Statistics for experimenters. In *Wiley Series in Probability and Statistics*. Wiley Hoboken, NJ, USA, 2005.

Aloke Dey and Rahul Mukerjee. *Fractional Factorial Plans*, volume 496. John Wiley & Sons, 2009.

Petros Drineas, Michael W Mahoney, Shan Muthukrishnan, and Tamás Sarlós. Faster least squares approximation. *Numerische Mathematik*, 117(2):219–249, 2011.

Arthur Fries and William G Hunter. Minimum aberration $2^{k-p}$ designs. *Technometrics*, 22(4):601–608, 1980.

Ulrike Grömping. R package frf2 for creating and analyzing fractional factorial 2-level designs. *Journal of Statistical Software*, 56(1):1–56, 2014.

Jens Hainmueller. Entropy balancing for causal effects: A multivariate reweighting method to produce balanced samples in observational studies. *Political Analysis*, 20(1):25–46, 2012.

A Samad Hedayat, Neil James Alexander Sloane, and John Stufken. *Orthogonal Arrays: Theory and Applications*. Springer Science & Business Media, 2012.

Kun Kuang, Peng Cui, Bo Li, Meng Jiang, and Shiqiang Yang. Estimating treatment effect in the wild via differentiated confounder balancing. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 265–274. ACM, 2017a.

Kun Kuang, Peng Cui, Bo Li, Meng Jiang, Shiqiang Yang, and Fei Wang. Treatment effect estimation with data-driven variable decomposition. In *AAAI*, pages 140–146, 2017b.

Kun Kuang, Peng Cui, Susan Athey, Ruoxuan Xiong, and Bo Li. Stable prediction across unknown environments. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pages 1617–1626. ACM, 2018.

Chang-Xing Ma and Kai-Tai Fang. A note on generalized aberration in factorial designs. *Metrika*, 53(1):85–93, 2001.

Ping Ma, Michael W Mahoney, and Bin Yu. A statistical perspective on algorithmic leveraging. *The Journal of Machine Learning Research*, 16(1):861–911, 2015.
Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-Correcting Codes*, volume 16. Elsevier, 1977.

Krikamol Muandet, David Balduzzi, and Bernhard Schölkopf. Domain generalization via invariant feature representation. In *Proceedings of the 30th International Conference on Machine Learning*, pages 10–18, 2013.

Jonas Peters, Peter Bühlmann, and Nicolai Meinshausen. Causal inference by using invariant prediction: identification and confidence intervals. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 78(5):947–1012, 2016.

Mateo Rojas-Carulla, Bernhard Schölkopf, Richard Turner, and Jonas Peters. Invariant models for causal transfer learning. *The Journal of Machine Learning Research*, 19(1):1309–1342, 2018.

Paul R Rosenbaum and Donald B Rubin. The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70(1):41–55, 1983.

Steven K. Thompson. *Sampling*. Wiley Series in Probability and Statistics. Wiley, 3 edition, 2012. ISBN 0470402318, 9780470402313.

Robert Tibshirani. Regression shrinkage and selection via the lasso. *Journal of the Royal Statistical Society: Series B (Methodological)*, 58(1):267–288, 1996.

Athanasios Tsanas, Max A Little, Patrick E McSharry, and Lorraine O Ramig. Accurate telemonitoring of parkinson’s disease progression by noninvasive speech tests. *IEEE Transactions on Biomedical Engineering*, 57(4):884–893, 2009.

HaiYing Wang. More efficient estimation for logistic regression with optimal subsamples. *The Journal of Machine Learning Research*, 20(132):1–59, 2019.

HaiYing Wang, Rong Zhu, and Ping Ma. Optimal subsampling for large sample logistic regression. *Journal of the American Statistical Association*, 113(522):829–844, 2018.

HaiYing Wang, Min Yang, and John Stufken. Information-based optimal subdata selection for big data linear regression. *Journal of the American Statistical Association*, 114(525):393–405, 2019.

CF Jeff Wu and Michael S Hamada. *Experiments: Planning, Analysis, and Optimization*, volume 552. John Wiley & Sons, 2011.

Hongquan Xu and CF Jeff Wu. Generalized minimum aberration for asymmetrical fractional factorial designs. *The Annals of Statistics*, 29(4):1066–1077, 2001.

Aijun Zhang, Kai-Tai Fang, Runze Li, Agus Sudjianto, et al. Majorization framework for balanced lattice designs. *The Annals of Statistics*, 33(6):2837–2853, 2005.

José R Zubizarreta. Stable weights that balance covariates for estimation with incomplete outcome data. *Journal of the American Statistical Association*, 110(511):910–922, 2015.