Appendix

A.1 ImageNet Model Details

We use the following models from Torchvision (details at https://pytorch.org/vision/0.8/models.html): alexnet [31], vgg11 [46], vgg11_bn, vgg13, vgg13_bn, vgg16, vgg16_bn, vgg19, vgg19_bn, resnet18 [18], resnet34, resnet50, resnet101, resnet152, squeezenet1_0 [27], squeezenet1_1, densenet121 [26], densenet169, densenet161, densenet201, googlenet [48], shufflenet_v2_x1_0 [32], mobilenet_v2 [43], resnext50_32x4d [53], resnext101_32x8d, wide_resnet50_2 [56], wide_resnet101_2, and mnasnet1_0 [49].


From the CLIP family [37], we use 33 models formed by weight-space interpolation between zero-shot and finetuned ViT-B/16, ViT-B/32, and ViT-L/14 (11 models from each architecture).

A.2 Pruning methods

In Section 4.1 we present results considering three categories of model pruning used in Diffenderfer et al. [8]: traditional (fine-tuning [16], gradual magnitude pruning [57]), rewinding lottery-tickets (weight-rewinding [12], learning-rate rewinding [42]), and initialization lottery-tickets (edgepopup [39], biprop [7]). Here we provide a brief description of each pruning method.

**Traditional.** As the name suggests, fine-tuning prunes a model at the end of the regular training period by removing $p\%$ of the weights with the smallest magnitude, then fine tunes the remaining weights using the learning rate at the end of the regular training period. Gradual magnitude pruning progressively removes weights during training in accordance with a sparsity scheduler (see Fig. 1 in Zhu and Gupta [57]) until the target sparsity is reached. Typically, some training takes place before and after pruning in gradual magnitude pruning.

**Rewinding lottery tickets.** Rewinding lottery tickets perform repeated training-then-pruning steps in which some percentage of the remaining weights are pruned at each pruning step (traditionally 20% of the remaining weights are pruned at each step). After each training-then-pruning step, either the weights and learning rate are rewound to their values at initialization (i.e. weight-rewinding) or the learning rate is rewound to a value earlier in the training process (learning-rate rewinding). The first rewinding lottery ticket method supported the Lottery Ticket Hypothesis [12] which suggests that sparse subnetworks exist within randomly initialized dense networks that can be trained to the same accuracy as dense networks.

**Initialization lottery tickets.** Stronger versions of this hypothesis, such as the Strong [39] and Multi-Prize Lottery Ticket Hypotheses [7] suggest that such subnetworks exist at initialization that achieve comparable accuracy to the dense network without requiring any training and, further, that these subnetworks’ weights can be binarized. Edgepopup identifies such subnetworks using surrogate scores to identify the most important weights at initialization. Biprop integrates weight and/or activation binarization into the search process for such subnetworks resulting in binary-weight or binary-weight and activation networks (BNNs). Note that biprop networks in this paper only make use of binarized weights.

A.3 Fourier interpolation on CIFAR-10 and computational details

Figure 1 in the main paper shows example Fourier amplitude and phase interpolating paths on ImageNet. Figure 6 shows example Fourier amplitude and phase interpolating paths on CIFAR-10, where again the images are rescaled for visualization (undoing the pixel-wise normalization).

Relatedly, note that in Section 3, the “lowest 40% of image frequencies” we reference is with respect to the maximum spatial frequency of the image (a function of the pixel resolution) and not based on
the actual power spectral density of the image. Further, the interpolation is done using a square mask on the DFT of the image, which interpolates the lower image frequencies but leaves the higher image frequencies unperturbed.

A.4 Jacobian norm computational details

We estimate the norm of the Jacobian using a random-projection-based approach that estimates the Jacobian norm as a function of a batch of samples of size $B$ and $n_{proj}$ projection vectors \[24\]. For CIFAR-10 and ImageNet, we set $n_{proj}$ to 10 and 50, respectively; we set $B$ to 400 and 1000, respectively. Error bars for our estimates are 95% confidence intervals constructed under the assumption that the $n_{proj}B$ unique Jacobian norm estimates made by the projection method are i.i.d., which is consistent with the error order of $(n_{proj}B)^{-\frac{1}{2}}$ expected by Hoffman et al. \[24\] when $B \gg 1$. Under this assumption, which may lead to underestimation of the true error if violated, our choice of $n_{proj}$ and $B$ ensures that the average error bar is less than 2% of the size of the estimated Jacobian norm (and all error bars are less than 8% of the size of the estimated Jacobian norm). Our estimated Jacobian norms are between 60 and 2300 for ImageNet models and between 2 and 50 for CIFAR-10 models.

A.5 Power spectral density of distribution shifts

To explore the behavior of models on OOD data, it is helpful to characterize the nature of the OOD data with respect to the ID test data; indeed this type of characterization is common practice \[55\]. Specifically, considering the difference in power spectral density (PSD) between each of the OOD test sets and the original ID test set allows us to categorize each OOD test set as being concentrated on low, mid, or high frequency perturbations with respect to the ID test set. We perform this characterization for CIFAR-10.1 and each of the 15 corruptions in CIFAR-10-C.

The PSDs shown in Figure 7 reflect the distribution shift between each OOD dataset and the original CIFAR-10 test set, and are sorted roughly in order of increasing frequency. Of note, this PSD characterization illustrates that the OOD shift encountered on CIFAR-10.1 data is composed of low-frequency information, much like the brightness and contrast CIFAR-10-C corruptions.

As each of the CIFAR-10-C corruptions are transformations applied to the original CIFAR-10 test images, the PSD for each CIFAR-10-C corruption is computed by taking the difference between each corrupted and original test image, computing the PSD of the resulting difference image, then averaging the PSDs for all images of the given corruption. As CIFAR-10.1 images are not corruptions of the original CIFAR-10 test images, the PSD characterization must be computed in a different manner. First, for each of the ten CIFAR-10 classes we compute the average PSD for CIFAR-10 test images and CIFAR-10.1 images and take the difference of these class PSDs. The final approximated PSD representing the CIFAR-10.1 shift is taken to be the average of the difference PSDs for the ten classes.
The dramatic variations in frequency content among these different distribution shifts underscore the difficulty of the robustness puzzle; models may need different tools or properties to achieve robustness on different types of distribution shifts.

Figure 7: Power spectral densities for low (CIFAR-10.1, brightness, contrast, fog, frost, snow), mid (elastic transform, motion blur, zoom blur, glass blur, defocus blur, pixelate, JPEG compression), and high (Gaussian noise, impulse noise, shot noise) frequency shifts with respect to CIFAR-10.

A.6 Pruning results on additional corruptions from CIFAR-10-C

Figure 8 and Table 5 extend Figure 2 and Table 1 to the nine remaining corruptions from CIFAR-10-C.
Figure 8: When does pruning affect OOD robustness?

Table 5: How well do metrics for pruned models correlate with OOD robustness?

A.7 Augmentation results on additional corruptions from CIFAR-10-C

Figure 9 and Table 6 extend Figure 3 and Table 2 to the nine remaining corruptions from CIFAR-10-C.
Figure 9: When does augmentation affect OOD robustness?

Table 6: How well do metrics for data-augmented models correlate with OOD robustness?

A.8 Best metric performance visualized for CIFAR-10 distribution shifts

Figures 10 and 11 visualize the fit to the data associated with the best metrics from the CIFAR-10 pruning analysis figures (Figures 2 and 8) and data augmentation analysis figures (Figures 3 and 9),
respectively. Note that Tables 7 and 8 are duplicates of the original figures' associated tables and are reproduced here for convenience.
Figure 10: When does pruning affect OOD robustness?

Table 7: Can model metrics explain why pruning affects OOD robustness?
- Gaussian Noise
- Contrast
- Pixelate
- Defocus Blur
- Phase - CD
- Pixel - between
- Pixel - within
- Phase - CD
- Phase - HFF
- Pixel - between
- Pixel - within
- Phase - CD
- ID accuracy
- Gaussian

- ID accuracy
- Gaussian
- Clean
- AugMix
- mR

<table>
<thead>
<tr>
<th>Clean</th>
<th>AugMix</th>
<th>Gaussian</th>
</tr>
</thead>
<tbody>
<tr>
<td>mR</td>
<td>mR</td>
<td>mR</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
<tr>
<td>0.91</td>
<td>0.92</td>
<td>0.91</td>
</tr>
</tbody>
</table>

- ID accuracy
- Gaussian
- Clean
- AugMix
- mR

<table>
<thead>
<tr>
<th>Clean</th>
<th>AugMix</th>
<th>Gaussian</th>
</tr>
</thead>
<tbody>
<tr>
<td>mR</td>
<td>mR</td>
<td>mR</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
</tbody>
</table>

- ID accuracy
- Gaussian
- Clean
- AugMix
- mR

<table>
<thead>
<tr>
<th>Clean</th>
<th>AugMix</th>
<th>Gaussian</th>
</tr>
</thead>
<tbody>
<tr>
<td>mR</td>
<td>mR</td>
<td>mR</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

- ID accuracy
- Gaussian
- Clean
- AugMix
- mR

<table>
<thead>
<tr>
<th>Clean</th>
<th>AugMix</th>
<th>Gaussian</th>
</tr>
</thead>
<tbody>
<tr>
<td>mR</td>
<td>mR</td>
<td>mR</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
<tr>
<td>0.47</td>
<td>0.54</td>
<td>0.54</td>
</tr>
</tbody>
</table>

- ID accuracy
- Gaussian
- Clean
- AugMix
- mR

<table>
<thead>
<tr>
<th>Clean</th>
<th>AugMix</th>
<th>Gaussian</th>
</tr>
</thead>
<tbody>
<tr>
<td>mR</td>
<td>mR</td>
<td>mR</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
<tr>
<td>-1.11</td>
<td>-1.25</td>
<td>-1.25</td>
</tr>
</tbody>
</table>

- ID accuracy
- Gaussian
- Clean
- AugMix
- mR

<table>
<thead>
<tr>
<th>Clean</th>
<th>AugMix</th>
<th>Gaussian</th>
</tr>
</thead>
<tbody>
<tr>
<td>mR</td>
<td>mR</td>
<td>mR</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
<tr>
<td>-0.64</td>
<td>-0.71</td>
<td>-0.71</td>
</tr>
</tbody>
</table>
**Figure 11:** When does augmentation affect OOD robustness?

**Table 8:** Can model metrics explain why augmentation affects OOD robustness?

### A.9 CLIP results on additional corruptions from ImageNet-C

Figure 12 and Table 9 extend Figure 4 and Table 3 to the remaining corruptions from ImageNet-C.
Table 9: How well do metrics for CLIP models correlate with OOD robustness?

<table>
<thead>
<tr>
<th>Metric</th>
<th>Non-CLIP</th>
<th>CLIP</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jacobian</td>
<td>1.37</td>
<td>0.68</td>
<td>0.40</td>
</tr>
<tr>
<td>Pixel + within</td>
<td>0.9</td>
<td>0.4</td>
<td>0.8</td>
</tr>
<tr>
<td>Pixel + between</td>
<td>-13.82</td>
<td>-0.82</td>
<td>-13.82</td>
</tr>
<tr>
<td>Amp + HFF</td>
<td>-12.88</td>
<td>-0.82</td>
<td>-12.88</td>
</tr>
<tr>
<td>Amp + CD</td>
<td>0.03</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>Phase + HFF</td>
<td>-13.08</td>
<td>-0.77</td>
<td>-13.08</td>
</tr>
<tr>
<td>Phase + CD</td>
<td>0.03</td>
<td>0.02</td>
<td>0.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metric</th>
<th>Non-CLIP</th>
<th>CLIP</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jacobian</td>
<td>1.74</td>
<td>-0.65</td>
<td>-0.7</td>
</tr>
<tr>
<td>Pixel + within</td>
<td>-17.76</td>
<td>-0.85</td>
<td>-17.76</td>
</tr>
<tr>
<td>Pixel + between</td>
<td>-16.24</td>
<td>-0.85</td>
<td>-16.24</td>
</tr>
<tr>
<td>Amp + HFF</td>
<td>-12.88</td>
<td>-0.85</td>
<td>-12.88</td>
</tr>
<tr>
<td>Amp + CD</td>
<td>0.03</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>Phase + HFF</td>
<td>-14.45</td>
<td>-0.70</td>
<td>-14.45</td>
</tr>
<tr>
<td>Phase + CD</td>
<td>0.03</td>
<td>0.02</td>
<td>0.00</td>
</tr>
</tbody>
</table>

A.10 ImageNet data augmentation results on all corruptions

Figures 5 and 13 and Tables 4 and 10 visualize the best metric for non-CLIP ImageNet models, including models from RobustBench [5] trained with data augmentation. Specifically, the RobustBench models are ResNet-50 models trained using the following data augmentations: Stylized-ImageNet [14], DeepAugment [22], and AugMix [21]. Importantly, our baseline models include a ResNet-50 trained without special data augmentations, allowing us to see the effect that the aforementioned data augmentations have on the predictability of robustness while holding architecture constant.

Similar to the robustness of CLIP models, the robustness of non-CLIP ImageNet models is often best predicted by our Fourier interpolation metrics (in particular, CD for amplitude interpolation does well in this setting). In-distribution accuracy can also show strong $R^2$, but it apparently has more trouble predicting the robustness of out-of-line models than our metrics. This phenomenon is illustrated on distribution-shifts like Pixelate and Gaussian Noise (see the corresponding rows of Figures 5 and 13), where in-distribution accuracy can predict many of the models’ robustnesses but clearly fails on the effectively robust models from RobustBench. Notably, in these cases, our amplitude CD metric can predict these effectively-robust models’ performances as well as it can predict the non-effectively-robust models’ performances.

Finally, we emphasize that, despite analyzing a variety of architectures, the out-of-line non-CLIP models on most distribution shifts are almost always the RobustBench models. Importantly, this is consistent with the focus on data augmentation for adding robustness [21, 14, 22], but it also suggests that the construction of architectures with effective robustness is a potential direction for future work.
Figure 13: When does ImageNet data augmentation affect OOD robustness?

Table 10: How well do metrics for ImageNet models correlate with OOD robustness?