A Note About Dual Norms

Used in Proof of Corollary 3.3 in *Efficient Neural Network Robustness Certification with General Activation Functions* by Zhang et al (NeurIPS 2018)

Corrolary 3.3's proof from paper

- From Appendix B of paper

$$\max_{\mathbf{x}\in\mathbb{B}_p(\mathbf{x_0},\epsilon)} f_j^U(\mathbf{x}) = \max_{\mathbf{x}\in\mathbb{B}_p(\mathbf{x_0},\epsilon)} \left[\mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x} + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)})\right]$$

$$= \left[\max_{\mathbf{x}\in\mathbb{B}_p(\mathbf{x_0},\epsilon)} \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x}\right] + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)})$$

$$\mathrm{y} = (1/\epsilon)\cdot(\mathbf{x} - \mathbf{x_0})$$

$$= \epsilon\left[\max_{\mathbf{y}\in\mathbb{B}_p(\mathbf{0},1)} \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{y}\right] + \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x_0} + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)})$$

Non-trivial part of proof

- From Appendix B of paper

$$\max_{\mathbf{x}\in\mathbb{B}_p(\mathbf{x_0},\epsilon)} f_j^U(\mathbf{x}) = \max_{\mathbf{x}\in\mathbb{B}_p(\mathbf{x_0},\epsilon)} \left[\mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x} + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)})\right]$$

$$= \left[\max_{\mathbf{x}\in\mathbb{B}_p(\mathbf{x_0},\epsilon)} \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x}\right] + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)})$$

$$= \epsilon\left[\max_{\mathbf{y}\in\mathbb{B}_p(\mathbf{0},1)} \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{y}\right] + \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x_0} + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)})$$

How ???

$$= \epsilon\|\mathbf{\Lambda}_{j,:}^{(0)}\|_q + \mathbf{\Lambda}_{j,:}^{(0)}\mathbf{x_0} + \sum_{k=1}^{m}\mathbf{\Lambda}_{j,:}^{(k)}(\mathbf{b}^{(k)} + \mathbf{\Delta}_{:,j}^{(k)}).$$

where $\frac{1}{p} + \frac{1}{q} = 1$

Crucial result used

Let $\mathbf{a} = (a_1, \ldots a_n)$ be a vector with p-norm $||\mathbf{a}||_p = \left(|a_1|^p + \cdots + |a_2|^p\right)^{\frac{1}{p}}$
The dual norm of $\mathbf{a} = \sup\{|\mathbf{a}^\top \cdot \mathbf{x}| \text{ s.t. } ||\mathbf{x}||_p \leq 1\}$

$||\mathbf{x}||_p \leq 1$ defines region of allowed $\mathbf{x}$
To maximize $\mathbf{a}^\top \cdot \mathbf{x}$, choose optimal $\mathbf{x}$ that has maximum projection on $\mathbf{a}$ in direction of $\mathbf{a}$.
Compute $\mathbf{a}^\top \cdot \mathbf{x} = a_1.x_1 + \cdots + a_n.x_n$ for optimal $\mathbf{x}$

For all $p \geq 1$, dual norm of $\mathbf{a} = ||a||_q$, where $\frac{1}{p} + \frac{1}{q} = 1$

Holder's Inequality (simplified)

Holder conjugates

Let $p, q \in [1, \infty]$ with $\frac{1}{p} + \frac{1}{q} = 1$

Then $\|\mathbf{a}^\top \cdot \mathbf{x}\|_1 \leq \|\mathbf{a}\|_q . \|\mathbf{x}\|_p$

$\sum_{i=1}^{n} |a_i . x_i| \leq \|\mathbf{a}\|_q . \|\mathbf{x}\|_p$

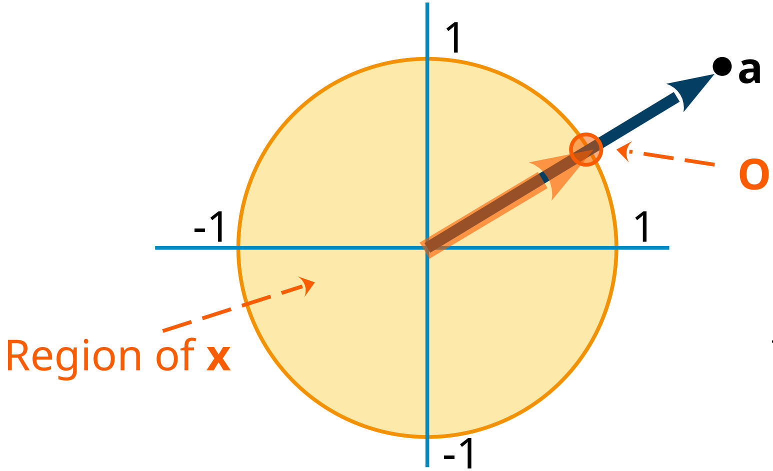
Some Illustrations of Result

- Consider 2 dimensional vectors
- Consider p-norms for $p = 1, 2, \infty$
- Corresponding q values: $\infty, 2, 1$ .... $1/p + 1/q = 1$

Not a proof; just some geometric intuition for simple cases

Playing with norms (p = 2, q = 2)

Let $\mathbf{a} = (a_1, a_2)$ be a fixed vector
Let $\mathbf{x} = (x_1, x_2)$ be a vector s.t. $||\mathbf{x}||_2 \leq 1$
i.e. $x_1^2 + x_2^2 \leq 1^2$
What is max value of $\mathbf{a}^\top \cdot \mathbf{x}$. i.e. $a_1.x_1 + a_2.x_2$?



Optimal x = $\frac{\mathbf{a}}{||\mathbf{a}||_2}$

Vector in region of **x** whose projection on **a** is maximum

$$\text{Max value of } \mathbf{a}^\top \cdot \mathbf{x} = \frac{||\mathbf{a}||_2^2}{||\mathbf{a}||_2} = ||\mathbf{a}||_2$$

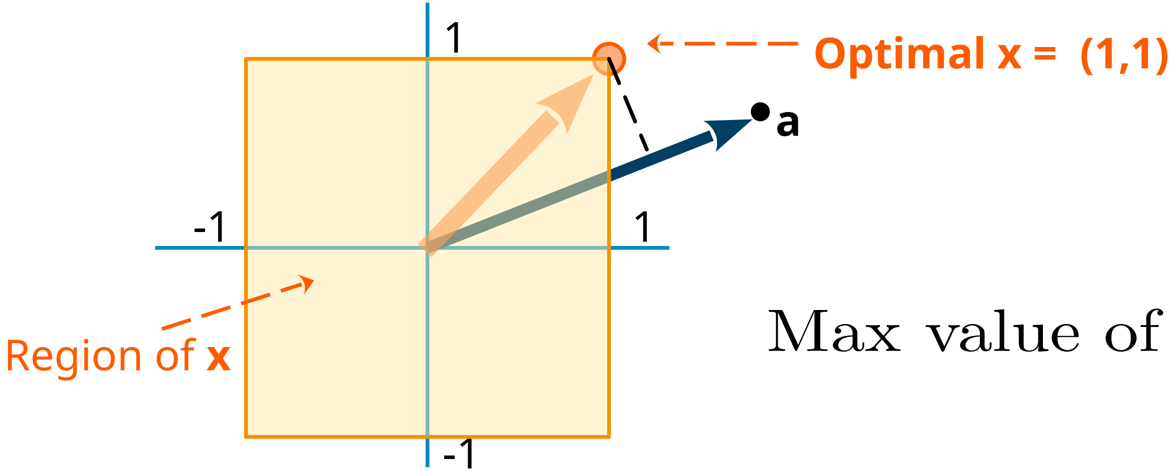
Playing with norms (p = ∞, q = 1)

Let $\mathbf{a} = (a_1, a_2)$ be a fixed vector

Let $\mathbf{x} = (x_1, x_2)$ be a vector s.t. $||\mathbf{x}||_\infty \leq 1$

i.e. $\max(|x_1|, |x_2|) \leq 1$

What is max value of $\mathbf{a}^\top \cdot \mathbf{x}$. i.e. $a_1.x_1 + a_2.x_2$?

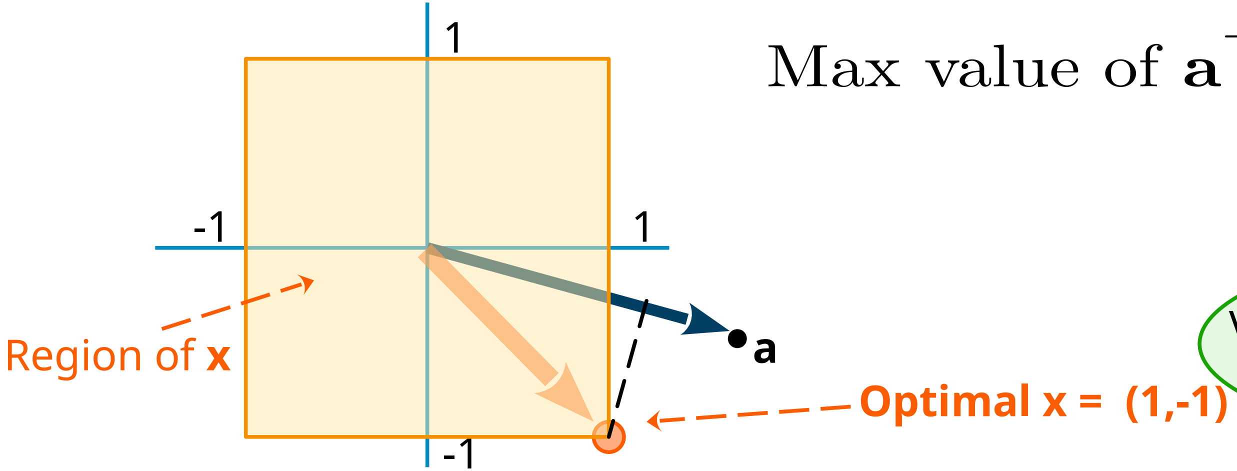


Vector in region of **x** whose projection on **a** is maximum

$$\text{Max value of } \mathbf{a}^\top \cdot \mathbf{x} = |a_1| + |a_2| = ||\mathbf{a}||_1$$

Playing with norms (p = ∞, q = 1)

Let $\mathbf{a} = (a_1, a_2)$ be a fixed vector
Let $\mathbf{x} = (x_1, x_2)$ be a vector s.t. $||\mathbf{x}||_\infty \leq 1$
i.e. $\max(|x_1|, |x_2|) \leq 1$
What is max value of $\mathbf{a}^\top \cdot \mathbf{x}$. i.e. $a_1.x_1 + a_2.x_2$?

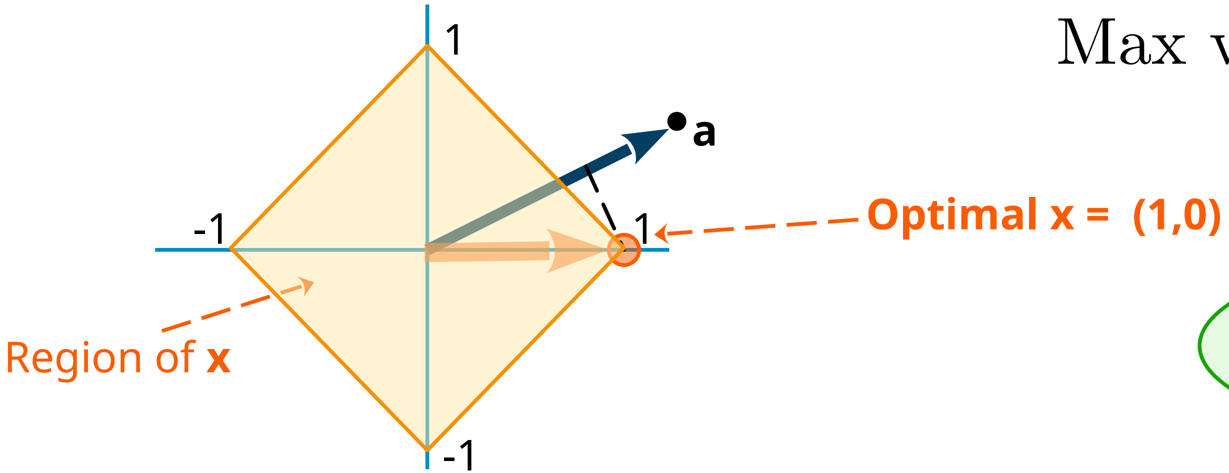


Max value of $\mathbf{a}^\top \cdot \mathbf{x} = |a_1| + |a_2| = ||\mathbf{a}||_1$

Vector in region of **x** whose projection on **a** is maximum

Playing with norms ($p = 1, q = \infty$)

Let $\mathbf{a} = (a_1, a_2)$ be a fixed vector
Let $\mathbf{x} = (x_1, x_2)$ be a vector s.t. $||\mathbf{x}||_1 \leq 1$
i.e. $|x_1| + |x_2| \leq 1$
What is max value of $\mathbf{a}^\top \cdot \mathbf{x}$. i.e. $a_1.x_1 + a_2.x_2$?



Max value of $\mathbf{a}^\top \cdot \mathbf{x} = |a_1|$
$= max(|a_1|, |a_2|) = ||\mathbf{a}||_\infty$

Vector in region of **x** whose projection on **a** is maximum

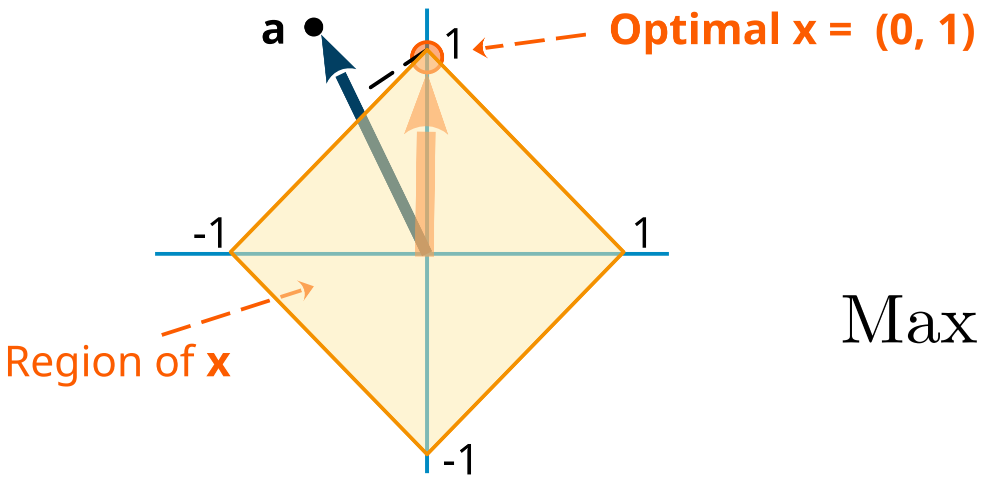
Playing with norms (p = 1, q = ∞)

Let $\mathbf{a} = (a_1, a_2)$ be a fixed vector

Let $\mathbf{x} = (x_1, x_2)$ be a vector s.t. $||\mathbf{x}||_1 \leq 1$

i.e. $|x_1| + |x_2| \leq 1$

What is max value of $\mathbf{a}^\top \cdot \mathbf{x}$. i.e. $a_1.x_1 + a_2.x_2$?



Vector in region of **x** whose projection on **a** is maximum

$$\text{Max value of } \mathbf{a}^\top \cdot \mathbf{x} = |a_2|$$
$$= max(|a_1|, |a_2|) = ||\mathbf{a}||_\infty$$