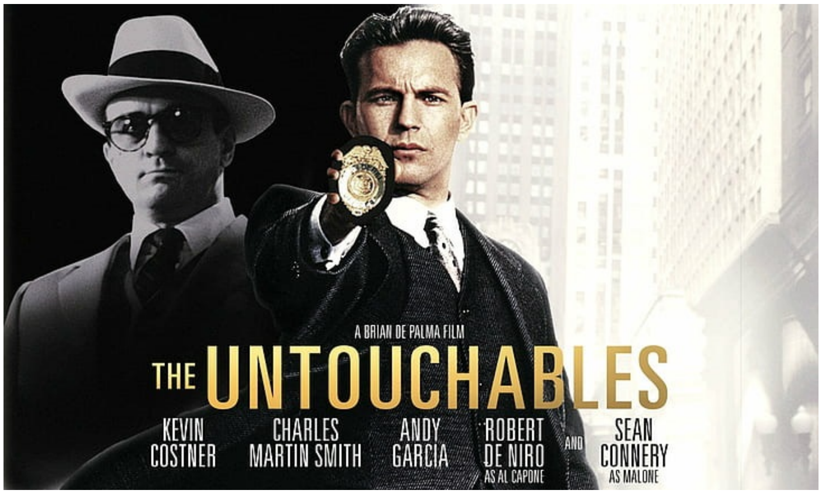
MATH 1800: Quantum Information Theory with Applications to Cryptography

Bonus 2



Consider the vector space of polynomials in one variable $V := \mathbb{k}[x]$, where $\mathbb{k} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ is the ground field. The vectors in V are polynomials $P(x) = a_0 + a_1 x + \ldots a_n x^n$ with $a_i \in \mathbb{k}$ and a natural basis is $e_n := x^n, n \in \mathbb{Z}_{\geq 0}$. For instance, $P(x) = 2 + x - x^2$ and $Q(x) = 1 - x^2 + 5x^4 - x^{10}$ are two typical vectors in V and the linear combination $3P(x) - 2Q(x) = 4 + 3x - x^2 - 10x^4 + 2x^{10}$ is in V as well. Next we enhance V with an inner product $\langle \cdot, \cdot \rangle$, s.t. the basis vectors $\{e_n\}_{n \in \mathbb{Z}_{\geq 0}}$ form an orthonormal basis:

$$\langle e_i, e_j \rangle = \delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j. \end{cases}$$

Recall that the **norm** of an operator $A : V \to V$ is given by

$$\|A\| := \sup_{v \in V} \frac{|Av|}{|v|} = \sup_{v \in V} \frac{\sqrt{\langle Av, Av \rangle}}{\sqrt{\langle v, v \rangle}}.$$

Problem 1 (2 pts) Find the norms of operators A below. If the norm is attained, give a vector $v \in V$ with $|Av| = \|A\| \cdot |v|$, otherwise explain why the norm is not attained on any vector.

(a) A is the operator of multiplication by x, i.e. $A(x^n) = x^{n+1}$.

(b) A is the linear operator given on the basis by $A(x^n) = \dfrac{n-1}{n} x^n$ for $n \geq 1$ and $A(1) = 1$.

Definition 1. A linear operator A from V to V is called **bounded** if there exists a number $C > 0$ such that for all $v \in V$

$$|Av| \leq C|v|.$$

Problem 2 (2 pts) Let $\mathcal{D} = \partial_x$ be the operator of differentiation with respect to x, i.e. $\mathcal{D}(x^n) = nx^{n-1}$. Is it bounded? If 'Yes', provide a number $C \in \mathbb{R}$ with $|\mathcal{D}v| \leq C|v|$ for any $v \in \mathbb{k}[x]$, if 'No', prove that such a number does not exist.

Problem 3 (1 pt) Watch movie 'The Untouchables' by Brian De Palma and write 'Yes' to claim the point.