2012 Putnam A5

Tristan Shin

11 Aug 2019

Let $\mathbb{F}_p$ denote the field of integers modulo a prime p, and let n be a positive integer. Let v be a fixed vector in $\mathbb{F}_p^n$, let M be an $n \times n$ matrix with entries of $\mathbb{F}_p$, and define $G : \mathbb{F}_p^n \to \mathbb{F}_p^n$ by $G(x) = v + Mx$. Let $G^{(k)}$ denote the k-fold composition of G with itself, that is, $G^{(1)}(x) = G(x)$ and $G^{(k+1)}(x) = G(G^{(k)}(x))$. Determine all pairs p, n for which there exist v and M such that the p^n vectors $G^{(k)}(0)$, $k = 1, 2, \dots, p^n$ are distinct.

The answers are $(p, 1)$ or $(2, 2)$ for any prime p. The former works with $(\mathbf{v}, M) = \left(\begin{bmatrix}1\end{bmatrix}, \begin{bmatrix}1\end{bmatrix}\right)$ while the latter works with $(\mathbf{v}, M) = \left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\right)$.

We work in $\mathbb{F}_p$. First, note by induction that $G^{(k)}(\mathbf{0}) = S_k\mathbf{v}$, where we define $S_k = I + M + M^2 + \ldots + M^{k-1}$ for $k = 1, \dots, p^n$. Now suppose $G^{(k)}(\mathbf{0})$ are distinct.

Define a function $\ell : \mathbb{F}_p^n \to \{1, \dots, p^n\}$ such that $G^{(\ell(\mathbf{u}))}(\mathbf{0}) = \mathbf{u}$ for any $\mathbf{u} \in \mathbb{F}_p^n$. Suppose that $\ell(\mathbf{0}) \neq p^n$. Then

$$G^{(\ell(\mathbf{0})+1)}(\mathbf{0}) = G(\mathbf{0}) = G^{(1)}(\mathbf{0})$$

contradiction. Thus $\ell(\mathbf{0}) = p^n$.

Now observe that for any $\mathbf{u} \in \mathbb{F}_p^n$,

$$\begin{aligned} S_{p^n}\mathbf{u} &= S_{p^n}G^{(\ell(\mathbf{u}))}(\mathbf{0}) \\ &= S_{p^n}S_{\ell(\mathbf{u})}\mathbf{v} \\ &= S_{\ell(\mathbf{u})}S_{p^n}\mathbf{v} \\ &= S_{\ell(\mathbf{u})}G^{(p^n)}(\mathbf{0}) \\ &= \mathbf{0} \end{aligned}$$

so $S_{p^n} = 0$. Thus the minimal polynomial of M divides $1 + x + x^2 + \ldots + x^{p^n-1} = (x-1)^{p^n-1}$. But note that $S_{p^{n-1}} \neq 0$ so the minimal polynomial does not divide $1 + x + x^2 + \ldots + x^{p^{n-1}-1} = (x-1)^{p^{n-1}-1}$ so it is $(x-1)^d$ for some $p^{n-1} \leq d \leq p^n - 1$. But also the minimal polynomial of M divides its characteristic polynomial by Cayley-Hamilton, and the characteristic polynomial has degree n, so $d \leq n$. Thus $p^{n-1} \leq n$. This easily implies $n = 1$ or $(p, n) = (2, 2)$ as desired. ■