Solution of a small problem

Ruicheng Hu 18071010131

September 23, 2025

First we translate it into a problem in linear algebra.

Set $k = \mathbb{F}_2$ be the finite field with two elements, consider the vector space $V = k^n$. For a given subset

$$A = \{a_1, a_2, \cdots, a_k\} \subset \{1, 2, \cdots, n\},$$

let α_A be the characteristic vector in V, i.e. the vector whose jth component is 1 if and only if $j \in A$. For any $1 \leq i \leq n$, put $\epsilon_i = \alpha_{\{i\}}$, i.e. the vector whose ith component is 1 and other components are 0. Let T be the linear transformation on V such that for any $1 \leq i \leq n$, $T\epsilon_i = \epsilon_{i+1}$ (here $\epsilon_{n+1} = \epsilon_1$)

Let $v \in V$ be the vetor which chracterizes the status of lamps, i.e. for any $1 \leq i \leq n$, the ith component of v is 1 if and only if the ith lamp is open. It is easy to see that when we press the jth button ($1 \leq j \leq n$), v changes into $v + T^j\alpha_A$. This means that a set A is good if and only if the vectors

$$T\alpha_A, T^2\alpha_A, \cdots, T^n\alpha_A$$

generates V. Since the map $A \mapsto \alpha_A$ is obviously bijective, we only need to count the number of vector α which satisfies that

$$T\alpha, T^2\alpha, \cdots, T^n\alpha$$

generates V. Such vectors will be called "good".

Let $R = k[x]$, then V is an R-module with x acting on it by T, i.e. $x \cdot v = Tv$ for $v \in V$. By the definition of T, it is easy to see that $T^n = \mathrm{id}_V$. Moreover $T^j\epsilon_1 = \epsilon_{j+1} (0 \leq j \leq n-1)$, so

$$\epsilon_1, T\epsilon_1, \cdots, T^{n-1}\epsilon_1$$

is a basis of V, which means $f(T) \neq 0$ for any nonzero polynomial $f \in R$ and $\deg f < n$. Therefore we conclude that T has the minimal polynomial $x^n - 1$, and then by the structure theorem we see $V \cong R/(x^n - 1)$ as R-modules.

Now a vector $\alpha \in V$ is good if and only if

$$\alpha, T\alpha, \cdots, T^{n-1}\alpha$$

(linearly) generates V, which is equivalent to that α is a generator of V as R-module. Note that $V \cong R/(x^n - 1)$ as R-modules and a generator in $R/(x^n - 1)$ (as R-module) is just a unit in the ring $R/(x^n - 1)$, we reduce to count the number of units in $R/(x^n - 1)$.

Let $n = 2^t \cdot m$ with $t \in \mathbb{N}$ and m an odd number, then $x^n - 1 = (x^m - 1)^{2^t}$ (in R). Since $x^m - 1$ is separable, we can decomposite it into distinct irreducible polynomials in R, say

$$x^m - 1 = \prod_{i=1}^{r} p_i(x). \tag{1}$$

Put $s = 2^t$ and $d_i = \deg p_i$; by Chinese remainder theorem we have

$$R/(x^n - 1) \cong \prod_{i=1}^{r} R/(p_i^s(x)),$$

then

$$(R/(x^n - 1))^\times \cong \prod_{i=1}^{r} (R/(p_i^s(x)))^\times, \tag{2}$$

so the required number is just $\prod_{i=1}^{r} |(R/(p_i^s(x)))^\times|$.

To compute $|(R/(p_i^s(x)))^\times|$, we use the fact that

$$(R/(p_i^s(x)))^\times = (R/(p_i^s(x))) \setminus (p_i(x) \cdot (R/(p_i^s(x)))).$$

Since p_i is irreducible, it is easy to check that the map $R/(p_i^{s-1}(x)) \to R/(p_i^s(x))$ which is given by $f \mapsto p_i \cdot f$ is an injection, and its image is just $p_i(x) \cdot (R/(p_i^s(x)))$. Note that for any polynomial $f \in R$, $R/(f(x))$ is a vector space over k of dimension $\deg f$, which means that

$$|R/(f(x))| = 2^{\deg f}.$$

Therefore we get

$$|(R/p_i^s(x))^\times| = |R/p_i^s(x)| - |p_i \cdot (R/p_i^s(x))| = |R/p_i^s(x)| - |R/p_i^{s-1}(x)| = 2^{sd_i} - 2^{(s-1)d_i} = 2^{(s-1)d_i}(2^{d_i} - 1).$$

Since $\sum_{i=1}^{r} d_i = m$ (by (1)) and (2), we get

$$|(R/(x^n - 1))^\times| = \prod_{i=1}^{r} (2^{(s-1)d_i}(2^{d_i} - 1)) = 2^{(s-1)m} \prod_{i=1}^{r} (2^{d_i} - 1). \tag{3}$$

The final step is to determine $d_i (1 \le i \le r)$ in the decomposition (1) of $x^m - 1$ in R. We need a standard result in the theory of finite fields; for completeness of the solution, we prove it as a lemma here.

Lemma. *Let γ be algebraic over k, and let u be the minimal positive integer such that $\gamma^u = 1$. Let l be the minimal positive integer such that $u | 2^l - 1$ (suppose u, l exist). Then the minimal polynomial of γ has degree l.*

Proof. Fix an algebraic closure $\bar{k}$ of k. Let d be the degree of the minimal polynomial of γ. We first prove that $d \le l$.

Let $E \subset \bar{k}$ be the unique extension of k with degree l, then E is the splitting field of the polynomial $x^{2^l} - x$ over k. Since $\gamma^u = 1$ and $u | 2^l - 1$, we have $\gamma^{2^l} = \gamma$, so $\gamma \in E$. Then

$$d = [k(\gamma) : k] \le [E : k] = l.$$

Now we prove that $d \ge l$. Consider the field $F = k(\gamma)$, we know that $[F : k] = d$, so F is a finite field with 2^d elements. This implies that $\gamma^{2^d} = \gamma$. By the minimality of u, we have $u | 2^d - 1$; then by the minimality of l, we see $d \ge l$.

In conclusion, we get $d = l$. □

Now consider the factorization of $x^m - 1$ (1). First we have

$$x^m - 1 = \prod_{v | m} \Phi_v(x), \tag{4}$$

where $\Phi_v(x)$ is the vth cyclotomic polynomial with degree $\phi(v)$. For any root γ of $\Phi_v(x)$ (in a fixed algebraic closure over k), $\gamma^v = 1$ since $\Phi_v(x)|x^v - 1$. For any $w < v$, since $x^w - 1$ and Φ_v are coprime over $\mathbb{Z}$, they are also coprime over k, which means $\gamma^w \neq 1$. So v is the minimal positive integer such that $\gamma^v = 1$. Since $v|m$, v is odd, so there exists a minimal positive integer l such that $v|2^l - 1$, denoted by $\mathrm{ord}_2(v) = l$. Then by the lemma, for any root γ of $\Phi_v(x)$, the minimal polynomial of γ over k has degree $\mathrm{ord}_2(v)$, which means that every irreducible polynomial in the decomposition of $\Phi_v(x)$ has degree $\mathrm{ord}_2(v)$.

Now apply the above discussion to the decomposition (1). By (4), for each $v|m$, there are $\frac{\phi(v)}{\mathrm{ord}_2(v)}$ number of d_i having value $\mathrm{ord}_2(v)$. Then by (3), we finally get the answer

$$2^{(2^t-1)m} \prod_{v|m} (2^{\mathrm{ord}_2(v)} - 1)^{\frac{\phi(v)}{\mathrm{ord}_2(v)}}, \tag{5}$$

where $n = 2^t m$ with $t \in \mathbb{N}$ and m an odd number.

When $n = p$ is an odd prime, we have $t = 0$ and $m = p$. By (5), the answer is simplified to be $(2^{\mathrm{ord}_2(p)} - 1)^{\frac{p-1}{\mathrm{ord}_2(p)}}$. I do not think this expression can be further simplified.