



کدهای دوری دوتایی ناشی از سه جمله‌ای جایگشت $f(x) = x + x^3 + x^{2^t+1}$ روی $GF(2^{2t-1})$

مژگان امامی

دانشگاه زنجان

محمدآزاد ویسی*

دانشگاه زنجان

چکیده

کدهای دوری زیرخانواده‌ای از کدهای خطی هستند که به دلیل داشتن الگوریتم‌های کدگذاری و کدگشایی کارآمد در مصارف الکترونیکی، سیستم‌های ذخیره‌سازی اطلاعات و سیستم‌های تبادل اطلاعات کاربرد دارند. در این مقاله، چندجمله‌ای $f(x) = x + x^3 + x^{2^t+1}$ روی $GF(2^{2t-1})$ را برای ساختن خانواده‌ای از کدهای دوری دوتایی به کار می‌گیریم و کرانی برای کمترین فاصله‌ی آن تعیین می‌کنیم. بیشتر کدهای ساخته شده در این مقاله بهینه هستند.

واژه‌های کلیدی: کدهای خطی، کدهای دوری، چندجمله‌ای جایگشت

Mathematics Subject Classification [2010]: 05B20

۱ مقدمه

فرض کنیم q توانی از عدد اول p باشد. α را عنصر اولیه‌ی میدان متناهی $GF(q)$ در نظر می‌گیریم. یک $[n, k, d]$ کد خطی روی $GF(q)$ زیرفضای k بعدی از $GF(q)^n$ با کمترین فاصله همینگ d است. یک $[n, k]$ کد خطی C روی میدان متناهی $GF(q)$ را دوری نامیم هرگاه $(c_0, c_1, \dots, c_{n-1}) \in C$ ایجاب کند که $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$. فرض کنیم $C = (g(x))$ یک کد دوری باشد، که $g(x)$ تکین و دارای کوچکترین درجه باشد، در این صورت $g(x)$ را چندجمله‌ای مولد C می‌نامیم. یک راه برای ساختن کدهای دوری روی $GF(q)$ از طول n استفاده از چندجمله‌ای مولد

$$\frac{x^n - 1}{\gcd(S^n(x), x^n - 1)} \quad (1)$$

است که $S^n(x) = \sum_{i=0}^{n-1} s_i x^i \in GF(q)[x]$ و $s^\infty = (s_i)_{i=0}^\infty$ یک دنباله با دوره‌ی تناوب n روی $GF(q)$ است. در این مقاله، کد دوری با چندجمله‌ای مولد (۱) را کد تولید شده توسط دنباله‌ی s^∞ نامیده و با C_s نمایش می‌دهیم. دنباله‌ی s^∞ را دنباله‌ی معرف کد دوری C_s می‌نامیم. در این مقاله، سه جمله‌ای جایگشت $f(x) = x + x^3 + x^{2^t+1}$ روی $GF(2^{2t-1})$ را برای ساخت رده‌ای از کدهای دوری دوتایی به کار خواهیم گرفت [۱] و کران پایینی برای کمترین وزن این کدها به دست می‌آوریم.

*سخنران