

مقدمه‌ای بر نظریهٔ کدگذاری

نگارش:

دکتر فرید (محمد) مالک قائینی

عضو هیأت علمی دانشکده ریاضی

انتشارات دانشگاه یزد

زمستان ۱۳۸۵



مالک قائینی، فرید محمد، ۱۳۳۲ -

مقدمه ای بر نظریه کدگذاری / نگارش فرید (محمد) مالک قائینی. - یزد: دانشگاه یزد، ۱۳۸۵.

۲۱۵ ص. : مصور، جدول.

ISBN 964 - 5808 - 58 - 8

۲۵۰۰۰ ریال:

واژه نامه

کتابنامه: ص. ۲۰۱.

نظریه رمز گذاری. دانشگاه یزد.

۷م / ۲م / ۲۶۸ / ۵۸

کتابخانه ملی ایران

۰۰۳ / ۵۴

۴۴۷۱۷ - ۸۵م

مرکز انتشارات دانشگاه یزد

یزد، صفائییه، بلوار دانشگاه، صندوق پستی: ۷۴۱ - ۸۹۱۹۵

تلفن: ۹ - ۸۲۱۱۶۷۰ دورنگار: ۸۲۱۰۶۹۹ - ۲۵۱

نام کتاب: مقدمه ای بر نظریه کدگذاری

نگارش: دکتر فرید (محمد) مالک قائینی

ناشر: انتشارات دانشگاه یزد

چاپ و صحافی: مؤسسه فرهنگی انتشاراتی بخشایش، ۷۷۳۷۵۸۳ - ۲۵۱

ویراستار: رویا درودی

نوبت چاپ: اول

تاریخ انتشار: بهار ۱۳۸۶

شمارگان: ۱۵۰۰

قیمت: ۲۵۰۰۰ ریال

ISBN 964 - 5808 - 58 - 8

شابک: ۹۶۴ - ۵۸۰۸ - ۵۸ - ۸

مرکز پخش: تهران، میدان انقلاب، کارگر جنوبی، خیابان وحید نظری، بین دوازدهم

فروردین و اردیبهشت، پلاک ۲۶۲، مؤسسه کتابیران تلفن: ۶۶۴۰۱۷۴۵ - ۲۱

پیش گفتار

در این کتاب مطالبی را ارائه داده‌ایم که افراد درگیر با مباحثی در زمینه‌های کامپیوتر و الکترونیک می‌توانند آنها را در طراحی سخت‌افزار و نرم‌افزارهای کامپیوتری به کار برده و از این طریق احتمال خطاپذیری سیستم مورد نظر خود را تا حد قابل قبولی کاهش دهند.

این کتاب براساس سرفصل‌های دو درس تهیه و تدوین شده است:

۱- درس نظریه کدگذاری رشته علوم کامپیوتر

۲- درس جبر کار بسته رشته ریاضی

و کلیه مباحث مربوط به کدهای تصحیح کننده خطا در این دو درس را پوشش می‌دهد و ولی مبحث رمزنگاری را مورد بحث قرار نمی‌دهد.

قسمت اعظم کتاب به بحث درباره کدهای خطی تصحیح کننده خطا می‌پردازد و تنها در فصل هشتم کتاب بحث مختصری درباره کدهای غیرخطی مطرح شده است. به علاوه بحث خود را به کدهای ثنائی محدود کرده‌ایم و این دو دلیل عمده دارد:

(الف) بحث درباره کدهای ثنائی ساده‌تر است، زیرا در این حالت تنها با دو نماد 0 و 1 سر و کار داریم و در نتیجه پیچیدگی ابزارهای جبری به کار گرفته شده را افزایش نمی‌دهد، و در عین حال افراد علاقه‌مند را آماده می‌سازد که برای مطالعه حالت کلی‌تر به متون دیگری که در بخش مراجع ذکر شده‌اند مراجعه نمایند.

(ب) سیستم‌هایی که این کدها بر روی آنها به کار گرفته می‌شوند ساختار ثنائی دارند.

اکنون به ذکر جزئیات بیشتری در مورد مطالب کتاب می‌پردازیم که خواننده را

در استفاده بهتر از کتاب یاری کند:

در مقدمه سعی کرده‌ایم با ارائه مثال‌هایی ساده و در عین حال جالب، انگیزه کافی را برای مطالعه فصول بعدی ایجاد کنیم. در فصل اول مقدمات جبری را ذکر کرده و در فصل دوم به معرفی میدان‌های متناهی پرداخته‌ایم. در واقع در فصل اول سعی کرده‌ایم برای خواننده آشنا با مفاهیم جبری پیشرفته، یک یادآوری از نظریه گالوا و توسیع میدان‌ها را ذکر کنیم تا او بتواند قسمت اعظم فصل دوم را به راحتی مطالعه کند و در عین حال از توانائی‌های خود برای ادامه کار اطمینان یابد. این فصل برای کسانی که دروس جبر خطی و جبر ۱ و ۲ را مطالعه کرده باشند ساده است و می‌توانند آنها را عمیقاً درک نمایند، ولی به خوانندگان ناآشنا با جبر توصیه می‌شود که در مطالعه اولیه خود فقط به مباحث بخش‌های (۱-۵) تا (۱-۸) پرداخته و سپس به سراغ مباحث فصل دوم بروند. در فصل دوم کوشیده‌ایم به نحوی نسبتاً مستقل از فصل اول و به روشی ساختنی (و نه وجودی) به مطالب مربوط به میدان‌های متناهی بپردازیم. برای مطالعه فصول سوم و چهارم، بخش کدهای ریتمولر از فصل پنجم و همچنین درک مطالب فصول هفتم و هشتم کتاب مطالعه بخش‌های (۲-۱) تا (۳-۲) کافی است. به علاوه برای مطالعه فصول کدهای دوری و کدهای گلی نیز مطالعه بخش‌های (۱-۲) تا (۸-۱) از فصل اول و بخش‌های (۲-۱) تا (۸-۲) از فصل دوم کافی می‌باشند. البته بخش بسیار زیبایی از کتاب که به حل و بحث معادلات درجه ۲ روی میدان‌های با مشخصه می‌پردازد و در بخش (۵-۲) برای مطالعه کدهای BCH دو تصحیح کننده مورد نیاز است در بخش‌های (۲-۹) تا (۲-۱۱) ارائه شده است. این بخش‌ها برای خواننده آشنا با جبر بسیار جالب و آموزنده هستند و خواننده ناآشنا با جبر می‌تواند در یک مطالعه اولیه این کتاب از آنها صرف‌نظر نماید. به هر حال حداقل زمینه لازم برای مطالعه قسمت اعظم این کتاب آشنایی با ابزارهای جبر خطی و ریاضیات گسسته است و از بقیه جهات نسبتاً خودکفاست. ضمناً در بسیاری موارد از ذکر اثباتها خودداری کرده‌ایم، زیرا دانستن اثبات‌ها بدون درک نحوه کاربرد مطالب توانایی خاصی را ایجاد نمی‌کند، ولی

در عین حال الگوریتم‌های مربوطه را ذکر کرده‌ایم زیرا به کمک آنها می‌توان مسائل را به روش ساختنی حل کرد و داشتن چنین توانایی‌هایی مفید است. در مواردی هم که اثباتی ذکر شده است انتهای اثبات را با علامت □ مشخص کرده‌ایم.

در خاتمه بر خود لازم می‌دانم که از استاد ارجمندم جناب آقای دکتر سید عبادا... محمودیان که راهنمایی‌های ارزنده‌شان باعث برطرف شدن برخی نقاط ضعف این کتاب شده است تشکری ویژه داشته باشم. از آقای دکتر سید محمود الهام‌بخش و سرکار خانم رویا درودی که زحمت بازبینی و ویرایش کتاب را تقبل فرمودند نیز سپاسگزارم. به علاوه لازم است از شورای محترم و ریاست انتشارات دانشگاه یزد سرکار خانم دکتر میرجلیلی که نقطه نظرات ارزشمندی را در جهت بهبود کیفیت این کتاب به اینجانب ارائه نمودند و همچنین سرکار خانم یوسفی مسئول محترم دفتر انتشارات دانشگاه یزد که زحمات زیادی را در ارتباط با این کتاب متحمل شده‌اند قدردانی نمایم. همچنین از آقای محمدمهدی صادقی‌نژاد که زحمت حروفچینی کامپیوتری کتاب را برعهده داشتند و در این زمینه زحمت زیادی کشیدند تشکر می‌کنم.

مسلماً این کتاب خالی از اشتباه و نقص نیست و مایه امتنان خواهد بود اگر خوانندگان این نوع اشتباهات و همچنین پیشنهادات و انتقاداتی که مسلماً می‌تواند باعث تکمیل تر شدن محتوای کتاب شود را به صورت کتبی یا از طریق پست الکترونیک «maalek@yazduni.ac.ir» به اطلاع اینجانب برسانند تا انشاء... برای چاپ بعدی بتوانیم آنها را در نظر داشته باشیم.

فرید (محمد) مالک قالینی

دانشگاه یزد - دانشکده ریاضی

فهرست مطالب

۱-۰	مقدمه	۱
۱-۰	چند مثال کاربردی	۱
۲-۰	مفاهیم بنیادی کدگذاری و نظریه اطلاعات	۵
۱۴	مسائل	
۱۵	۱ مقدمات جبری	
۱۵	۱-۱ مقدمه	
۱۵	۲-۱ گروه	
۱۷	۳-۱ حلقه	
۱۸	۴-۱ ایده آل	
۱۹	۵-۱ میدان	
۲۲	۶-۱ فضای برداری	
۲۶	۷-۱ معادلات خطی	
۳۰	۸-۱ تبدیلات خطی	
۳۲	۹-۱ توسیع میدانها	
۳۵	مسائل	
۳۷	۲ میدانهای منتهای	
۳۷	۱-۲ مقدمه	
۳۸	۲-۲ کلیات	
۴۱	۳-۲ نظریه اساسی میدانهای منتهای	
۴۵	۴-۲ چندجمله‌ای‌های کمین	
۵۶	۵-۲ یافتن چندجمله‌ای‌های تحویل ناپذیر	

۵۹	جداول برخی از میدان‌های کوچک
۶۵	گروه خودریختی‌های $GF(p^m)$ روی $GF(p)$
۶۸	تعداد چندجمله‌ای‌های تحویل‌ناپذیر
۶۹	پایه‌های $GF(p^m)$ روی $GF(p)$
۷۲	معادلات درجه دوم روی $GF(2^m)$
۷۶	بستار جبری
۷۹	مسائل
۸۵	۳ کدهای تصحیح‌کننده خطا
۸۵	۱-۳. مقدمه
۸۶	۲-۳. کدهای تصحیح‌کننده خطا
۹۰	مسائل
۹۱	۴ آشنایی با کدهای خطی
۹۱	۱-۴. مقدمه
۹۱	۲-۴. نظریه عمومی کدهای خطی
۱۰۲	۳-۴. ساختن کدهای جدید بر مبنای یک کد خطی مفروض
۱۰۸	۴-۴. برخی شرایط لازم برای وجود یک کد خطی $[n, k, d]$
۱۱۱	مسائل
۱۱۷	۵ برخی کدهای خطی مهم دیگر
۱۱۷	۱-۵. مقدمه
۱۱۷	۲-۵. کدهای ۲- تصحیح‌کننده BCH
۱۲۳	۳-۵. کدهای رید-مولر
۱۳۵	مسائل

۱۳۷	۶ کدهای دوری
۱۳۷	۱-۶. مقدمه
۱۳۹	۲-۶. کدهای دوری به عنوان ایده آل
۱۴۴	۳-۶. برخی کدهای دوری مهم
۱۴۷	۴-۶. چندجمله‌ای آزمون
۱۴۹	۵-۶. کدهای t-تصحیح کننده دوری
۱۵۲	۶-۶. کد گلی
۱۵۸	۷-۶. کشف و تصحیح خطا در کدهای دوری
۱۵۹	مسائل
۱۶۱	۷ کدهای غیرخطی
۱۶۱	۱-۷. مقدمه
۱۶۲	۲-۷. کلیات
۱۶۴	۳-۷. کران پلاتکین
۱۶۸	۴-۷. ماتریس‌های آدامار و کدهای ناشی از آنها
۱۷۵	۵-۷. قضیه لونشتاین
۱۷۸	۶-۷. کدهای ناشی از طرح‌ها
۱۸۲	۷-۷. کد کردن و کدگشایی در کدهای غیرخطی
۱۸۴	مسائل
۱۸۷	۸ کدهای روی گراف‌ها
۱۸۷	۱-۸. مقدمه
۱۸۷	۲-۸. مفاهیم اساسی مبحث گراف‌ها
۱۸۹	۳-۸. کدهای یالی گراف‌ها

۱۹۱	۴-۸ کدهای راسی گراف‌ها
۱۹۵	۵-۸ کدهای ۱- کامل در حاصل ضرب گراف‌ها
۱۹۸	۶-۸ کدهای ۱- کامل روی گراف‌های دوپارچه کامل
۲۰۰	مسائل
۲۰۱	فهرست منابع
۲۰۲	فهرست راهنما
۲۰۵	واژه‌نامه فارسی به انگلیسی
۲۱۰	واژه‌نامه انگلیسی به فارسی
۲۱۵	برخی نمادهای مهم کتاب