

اصول کدهای تصحیح کننده‌ی خطا

مترجم: دکتر ناصر زمانی

سروشنامه	هافمن، ویلیام کری، ۱۹۳۱-م.
عنوان و نام پدیدآور	Huffman, W. C. (William Cary)
مشخصات نشر	اصول کدهای تصحیح کننده ی خطا
مشخصات ظاهری	تهران : آموزشهای بنیادی، ۱۳۹۴.
شابک	۹۷۸-۶۰۰-۷۰۵۹-۱۸-۰
وضعیت فهرست نویسی	۴۱۳ ص.
یادداشت	فهرست مختصر
یادداشت	فهرست نویسی کامل این اثر در نشانی http://opac.nliai.ir قابل دسترسی است
شناسه افزوده	عنوان اصلی: fundamentals of error correcting codes:
شناسه افزوده	بلاس، ویرا
شماره کتابشناسی ملی	رمانی، ناصر، ۱۳۴۹
	۳۸۱۶۴۴۲

کتابخانه

نام کتاب: اصول کدهای تصحیح کننده ی خطا

تالیف: دکتر ناصر زمانی

سال چاپ / نوبت چاپ / تیراژ: ۱۳۹۴ / اول / ۱۰۰۰

قیمت: ۲۵۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۷۰۵۹-۱۸-۰

تلفن دفتر نشر: ۶۶۰۱۹۱۰۷ Email: m@abnashr.com www.abnashr.com

تهران- میدان جمهوری- جنب مترو نواب- برج شهاب ۱- طبقه پنجم- شماره ۱۵۶

فهرست مندرجات

۷	بیشگفتار
۱۱	بیشگفتار مترجم
۱۳	۱ مفاهیم بنیادی کدهای خطی
۱۵	۱.۱ سه نوع مبدائی
۱۶	۲.۱ کدهای خطی، ماتریس‌های مولد و کنترل‌توان
۱۸	۳.۱ کدهای دوگان
۲۰	۴.۱ وزن‌ها و فواصل
۲۷	۵.۱ ساختن کدهای جدید از قبلی
۲۷	۱.۵.۱ سوراخ کردن کدها
۲۸	۲.۵.۱ توسعه کدها
۳۱	۳.۵.۱ کوتاه کردن کدها
۳۳	۴.۵.۱ جمع‌های مستقیم
۳۳	۵.۵.۱ ساختن 2^m و 2^{m-1}
۳۴	۶.۱ کدهای هم‌ارز حابکستی
۳۹	۷.۱ هم‌ارزی کلی‌تر کدها

۸.۱ کدهای همبند ۴۵

۹.۱ کدهای گوی ۴۸

۱.۹.۱ کدهای نوی دودویی ۴۸

۲.۹.۱ کدهای گوی سه‌سه‌ای ۵۰

۱۰.۱ کدهای رید-مولر ۵۱

۱۱.۱ گذشانی، گذشانی و فاصله شش ۵۴

۱.۱.۱ گذشانی ۵۵

۲.۱.۱ گذشانی و فاصله شش ۵۷

۱۲.۱ گران بسته‌ای کد، شعاع پوششی و کدهای کامل ۶۸

۲ گران‌ها روی اندازه کدها ۷۵

۱.۲ $1, 1, 1, 1$ و $1, 1, 1, 1, 1, 1$ ۷۵

۲.۲ گران بالای پلانکس ۸۱

۳.۲ گران‌های بالای جاسون ۸۴

۱.۳.۲ گران جاسون مقید ۸۵

۲.۳.۲ گران جاسون بی‌قید ۸۷

۳.۳.۲ گران جاسون برای 1 ۸۹

۴.۳.۲ کد بردار استروم-رایسون ۹۳

۵.۳.۲ کدهای دوری غربی کامل ۹۵

۴.۲ گران بالای سنکلیون و آ.های VDS ۹۷

۵.۲ گران بالای تپاس ۹۹

۶.۲ کران بالایی برنامه ریزی خطی ۱۰۲

۷.۲ کران بالایی کریسپر ۱۰۹

۸.۲ کران پایین زیلیت ۱۱۶

۹.۲ کران پایین ورتاموف ۱۱۷

۱۰.۲ کران های محاسباتی ۱۱۹

۱۰.۱.۲ کران سینکلتون محاسباتی ۱۲۰

۱۰.۲.۲ کران پلانگین محاسباتی ۱۲۰

۱۰.۲.۳ کران همینگ محاسباتی ۱۲۱

۱۰.۲.۴ کران الیاس محاسباتی ۱۲۴

۱۰.۲.۵ کران های AIRRW ۱۲۵

۱۰.۲.۶ کران زیلیت ورتاموف محاسباتی ۱۲۶

۱۱.۲ کدهای قاموسی ۱۲۷

۳ میدان های منتهای ۱۳۳

۱.۳ مقدمه ۱۳۳

۲.۳ جند حمله ای ها و الگوریتم اقلیدسی ۱۳۵

۳.۳ نصوص های اولیه ۱۳۸

۴.۳ ساختن میدان های منتهای ۱۴۰

۵.۳ زیر میدان ها ۱۴۵

۶.۳ انومرفیسم های میدان ۱۴۷

۷.۳ همبسته های دایره ای و جند حمله ای های مستقیم ۱۴۸

- ۸.۳ رد و وریدهای زیرمعدانی ۱۵۳
- ۴ کدهای دوری ۱۵۹
- ۱.۴ تجربه ۱ ۱۶
- ۲.۴ نظریه سادگی کدهای دوری ۱۶۳
- ۳.۴ جویهای ها و برکنرها ۱۷۲
- ۴.۴ حفرهای یک کد دوری ۱۸۴
- ۵.۴ منبهم و حمله کدهای دوری ۱۹۶
- ۶.۴ کدگذاری کدهای دوری به روش مجت ۲۰۴
- ۷.۴ کدهای لای-آمن ۲۱
- ۵ کدهای BCH و رید-سلمن ۲۱۷
- ۸.۵ کدهای BCH ۲۱۷
- ۲.۵ کدهای رید-سلمن ۲۲۴
- ۳.۵ کدهای رید-سلمن تعمیم یافته ۲۲۷
- ۴.۵ کدگذاری کدهای BCH ۲۳۱
- ۱.۴.۵ کدگذاری پیرسون-کرسن-ریز ۲۳۱
- ۲.۴.۵ کدگذاری پیرسون-کرسن-ریز ۲۴۱
- ۳.۴.۵ کدگذاری پیرسون-کرسن-ریز ۲۴۵
- ۴.۴.۵ کدگذاری پیرسون-کرسن-ریز ۲۵۱

۲۵۸ ۵.۵ خطاهای ریشه‌ای، گدهای تجربی و لایه‌بندی

۲۶۲ ۶.۵ کدگذاری لوح فشرده

۲۶۲ ۱.۶.۵ کدگذاری

۲۶۶ ۲.۶.۵ کدکشی

۲۶۹ ۶ گدهای دوتایی

۲۶۹ ۱.۶ تعریف و خواص اصلی

۲۷۹ ۲.۶ کمی نظریه اندازه

۲۸۲ ۳.۶ وجود گدهای دوتایی

۲۸۶ ۴.۶ تعامد گدهای دوتایی

۲۹۵ ۵.۶ وزن‌ها در گدهای دوتایی

۳۰۴ ۶.۶ گدهای مانده درجه دوم

۳۰۷ ۱.۶.۶ گدهای QR روی میدان‌های نامشخصه ۲

۳۱۱ ۲.۶.۶ گدهای QR روی میدان‌های نامشخصه ۳

۳۱۴ ۳.۶.۶ توسعه گدهای QR

۳۱۹ ۴.۶.۶ اتورم‌های گدهای QR توسعه یافته

۳۲۲ ۷ توزیع‌های وزنی

۳۲۳ ۱.۷ معادلات مک و بلانکر

۳۲۶	۲.۷ فرمول‌بندی‌های هم‌اوز
۳۳۱	۳.۷ یک نتیجه یکتایی
۳۳۵	۴.۷ گدهای AIDS
۳۳۹	۵.۷ توزیع‌های ورتی همدسته‌ای
۳۴۶	۶.۷ توزیع‌های گدهای سوراخ‌سده و کوتاه‌سده
۳۴۹	۷.۷ شمار شماری‌های ورتی
۳۵۱	۸.۷ نمود رتبی ورتی‌ها
۳۵۶	۹.۷ سبب‌های حافظ ورتی
۳۶۱	۱۰.۷ ورتی‌های همبستگی تعیین‌یافته
۳۸۵	واژه‌نامه انگلیسی به فارسی
۳۹۵	واژه‌نامه فارسی به انگلیسی
۴۵	فهرست الفبایی و نمادها
۴۵	واژه‌نامه فارسی به انگلیسی

پیشگفتار

نظریه کد در سال ۱۹۴۸ با انتشار مقاله "یک نظریه ریاضی ارتباطات" توسط کلود شانون شروع شد. در نیم قرن گذشته، نظریه کدگذاری به شاخه‌ای میان رشته‌ای بین ریاضیات و مهندسی با کاربردهایی در تقریباً همه زمینه‌های ارتباطات مانند انتقال مخابراتی و تلفن همراه، ثبت لوح فشرده و ذخیره‌سازی داده‌ها رشد یافته است.

در ادامه سالگرد مقاله بنیادی شانون، کتاب دو جلدی راهنمای نظریه کدگذاری، که توسط نویسندگان کتاب حاضر ویرایش شده است، توسط انتشارات ایلر ویرس منتشر چاپ شد. این کتاب راهنمای مشارکت ۳۲ مولف، حوزه وسیعی از بحث‌ها را در مباحثات پژوهشی پوشش می‌دهد. به عنوان ویراستار، آن کتاب، تدوین یک کتاب درسی کمکی را احساس کردیم. هدف این کتاب درسی مقدمه‌ای عمیق در نظریه کد از نقطه‌نظرهای ریاضی و مهندسی بود که برای مدریس یا محصلان افرادی مناسب باشد. بیشتر بحث‌ها، موضوعات رایج هستند، گرچه برخی از آنها موضوعات موجود در کتاب‌ها و مجلات تخصصی را پوشش می‌دهند. امیدواریم نگارش این کتاب، با مثال‌ها و تمرینات متعدد، مقدمه‌ای قابل فهم ارائه کرده و خواننده را برای غقیب برخی از موضوعات کدگذاری توانمند سازد.

کتاب اصول کدهای تصحیح کننده خطا عمدتاً یک کتاب درسی خودکفاست که برای دانشجویان سال آخر لیسانس و دانشجویان فوق لیسانس مناسب است. پس از آن درسی در حیطه خطی است. گرچه ضروری نیست ولی درسی نیز در حیطه غیر خطی است. این کتاب می‌تواند برای حداقل سه ترمسال تحصیلی استفاده شود. انواع مثال‌ها، نظریه و محاسبات را بررسی می‌کنند و پس از ۸۵ تمرین در محلی‌های مناسب کتب درج شده‌اند. اغلب نظریه یا اثبات کامل همراه است و برخی از اثبات‌ها به تمرینات واگذار شده‌اند. به دلیل کثرت مثال‌ها و تمرینات که نظریه را بررسی می‌کند، ن‌کند، عدم تأکید به اثبات‌ها در اختیار مدریس است.

در این پیشگفتار به طور مختصر محتوای ۷ فصل کتاب را توصیف کرده و یک طرح پیشنهادی برای اولس نیمسال ارائه می‌دهیم. فصل ۱، مقدمه‌ای در کدهای خطی، مدریس‌های مؤلف و کنترل توان، کدهای دوکان، وزن و فاصله، کدگذاری و گذرسانی و گران سیمه‌ای گرد، اساسی است. کدهای همبند، کدهای کوئی، کدهای رینگ دو دویی و شش‌تد معرفی می‌شوند. قضیه شانون برای کانال متغیر دو دویی بحث می‌شود. فصل ۲ برای درک شتاب کتاب مهم است.

فصل ۳، اثران‌های بالا و پایین مهم را بر روی اندازه کدهای خطی و غیرخطی پوشش

می‌دهد. اینها شامل گران‌های بلانکین، جانسون، سینگلتون، الیاس، برنامه‌ریزی خطی، کریسمر، زیلبرت و ورشاموف هستند. نسخه‌های محاسباتی اکثر این گران‌ها آورده می‌شوند. کدهای AIDS و گدهای فاموسی معرفی می‌شوند.

فصل ۳ مقدمه‌ای برای ساختن و خواص میدان‌های متناهی است که برخی از اثبات‌ها حذف می‌شوند. اگر دانشجویان با ساختن میدان‌های متناهی، چندجمله‌ای‌های تحویل نابدر، تجربه چندجمله‌ای‌ها روی میدان‌های متناهی و نظریه کالوای میدان‌های متناهی آشنا باشند، پرداختن سریع به این فصل ممکن است. بیشتر فصل ۳ فوراً در فصل ۴ برای مطالعه کدهای دوری استفاده می‌شود. حتی با وجود زمینه آسانی با میدان‌های متناهی ممکن است همدسته‌های دایره‌ری (بخش ۷.۳) برای دانشجوی تازه باشد.

فصل ۴ نظریه اساسی کدهای دوری را ارائه می‌کند. نحوه ارائه‌مان، مفاهیم مولد خودتوان، چندجمله‌ای مولد، صفرهای یک‌گانه و مجموعه‌های معرف را به هم مرتبط می‌کند. ضرب‌گرها را برای کشف هم‌ارزی کدهای دوری به کار می‌بریم. گزینشی محبت کدهای دوری بر همانند کدهای دوری توسعه‌یافته و گدهای پایانی آفیس معرفی می‌شوند.

فصل ۵ به خانواده‌های خاص کدهای BCH و رند-سلسن دوری و کدهای رند-سلسن تعمیم‌یافته می‌پردازد. چهار الگوریتم گزینشی برای این کدها ارائه می‌شوند. خطاهای رشته‌ای و روش اتصال در مورد مبهم خطاهای رشته‌ای با کاربرد از این ایده‌ها در استفاده از کدهای رند-سلسن در گذرکداری و گزینشی لوح‌های فشرده معرفی می‌شوند.

در ادامه نظریه کدهای دوری، فصل ۶ نظریه کدهای دوری دوبابی را ارائه می‌کند که شامل خانواده کدهای مانده درجه دوم هستند. چون نظریه کامل کدهای مانده درجه دوم صرفاً کمی ساده‌تر از نظریه کدهای دوبابی است، نظریه این کدهای دوبابی را معرفی کرده و سپس آن را در مورد کدهای مانده درجه دوم به کار گرفته‌ایم. خودتوان‌های کدهای مانده درجه دوم دوبابی و سه‌سه‌ای ضرب‌محاسبه شده‌اند. در صفحه‌های تصویبی به عنوان مثال‌هایی از طرح‌های ترکیبیاتی حاصل از گذرکدهای از یک وین ثابت در یک معرفی می‌شوند.

فصل ۷ مفهوم توزیع ورتی تعریف شده در فصل ۶ را توسعه می‌دهد. شش شکل معادل اتحادهای مک‌ویلیامز، انجم از گسترده‌های دوبابی باشد، که توزیع‌های ورتی یک‌گانه و دوگانه آن را مرتبط می‌کنند، فرمول‌بندی می‌شوند. کدهای AIDS که در فصل ۲ و توزیع‌های ورتی همدسته که در فصل ۶ معرفی شدند، هستند و دوباره بررسی می‌شوند. اثباتی از یک قضیه مک‌ویلیامز در مورد تبدیلات حافظ ورتی، در بخش ۹.۷ ارائه می‌شود.

فصل‌ها و بخش‌های زیر از این کتاب به عنوان یک درس یک ترمی در نظریه گذرکدهای معرفی می‌شوند:

• فصل ۶ (به جز بخش ۷.۱)

• بخش‌های ۱.۲، ۲.۳، ۳.۴، ۴.۲، ۷.۲، ۹.۲

- فصل ۳ (به جز بخش ۸.۳)
- فصل ۴ (به جز بخش‌های ۶.۴ و ۷.۴)
- فصل ۵ (به جز بخش‌های ۳.۴.۵، ۴.۴.۵ و ۵.۵ و ۶.۵) و
- بخش‌های ۱.۷ و ۳.۷

اگر ارائه درس دیگری در نظریه گذ ممکن باشد، موضوعات فصل ۷ می‌تواند با دو بخش آخر فصل ۵ جایگزین شوند. این مواد چگونگی گذگذاری و گذگشایی نوع‌های فشرده را نشان می‌دهند که یک کاربرد خوب و مبتنی است که دانشجویان می‌توانند با آن سر و کار داشته باشند.

علاقه‌مندیم از فلبلیت کالوریت که بخش‌هایی از کتاب حاضر را در قالب درسی در نظریه گذگذاری در دانشگاه اینلینور سیکاگو بررسی کرده و منجر به ارائه ایده‌های مفیدی شده است، قدردانی نماییم. وی همچنین برخی از داده‌های جدول فصل ۳ را آماده کرده است. همچنین از کارکنان و همکاران انتشارات دانشگاه کمبریج به خاطر مساعدت‌های ارزشمند در تولید این کتاب تشکر می‌کنیم. مخصوصاً از مدیر ویرایش دکتر فلیت مبلر، ویراستار کنیز دکتر لسللی حلی، بوماس و ویراستار تولید خانم لوسل موریانی قدردانی می‌کنیم. به ویژه علاقه‌مندیم از دانشجویان خود در درس‌های نظریه گذ تشکر کنیم که سؤالات و پیشنهاد‌های آنها به پیراستگی متن کمک نمود. مخصوصاً جان لارک کیم از دانشگاه اینلینور سیکاگو و روبین کابینگ از دانشگاه لویولای سیکاگو بسیار باری بخش بودند. با هدف حذف حاشاها، برای خواندن و ترجمانی متن، کنترل مثال‌ها و انجمن تمرینات توجه زیادی نموده‌ایم. ولی مانند همه کتاب‌ها احتمالاً خطه‌هایی وجود دارند، از هرگونه تصحیحی که خواستگاران ارائه دهند استقبال کرده و در آدرس‌های زیر قابل دسترسی هستیم.

W. Cary Huffman

web@math.uchicago.edu

Vera Pless

pless@math.uchicago.edu

پیشگفتار مترجم

کتاب اصول کدهای تصحیح‌کننده خطا نوشته هافمن و پلنس در میان متخصصین کدگذاری کتاب‌ناشناخته‌ای نیست. کتابی است جامع در نظریه کدگذاری که محتوای علمی و سطح دقت در ارائه مطالب آن را از کتاب مسیحه‌ساز ساخته است.

به علاوه، شیوه نگارش، ترتیب و تنوع مطالب در آن طوری است که نه تنها برای تدریس در رشته‌های ریاضی و فنی مهندسی مناسب‌ترین کتاب است بلکه به عنوان یک کتاب مرجع مورد استفاده پژوهشگران است. نظریه اهمیت این کتاب و همچنین احساس نیاز مبرم دانشجویان به متن فارسی این اثر ارزنده تصمیم به ترجمه آن گرفته و اینک با افتخار و مسرت ترجمه هفت فصل اول از کتاب مذکور را در قالب جلد اول به نام «ملاقیه مبتدیان» می‌نمایم. بدیهی است که فهرست مطالب، پیشگفتار نویسندگان و منابع موجود در آخر کتاب مناسب با هفت فصل ترجمه‌شده بعدی تنظیم شده و صرفاً موارد مرتبط با این هفت فصل گردانده شده‌اند. در ترجمه متن تلاش شده است علاوه بر رعایت امانت، حملات به فارسی روان و ساده ارائه شوند. لازم به ذکر است که برخی از واژه‌های موجود در کتاب برای مترجم نادرگی داشته است و با اینکه تلاش زیادی شده است با واژه‌های معادل انتخاب شده به قدر کافی مناسب و رسا باشد تردید داریم که همه آنها مطلقاً سلیقه همه خوانندگان باشند. امید است خوانندگان هرگونه اشتباه یا انحراف در ترجمه را گوشزد نمایند تا در چاپ‌های بعدی اصلاح شوند.

از خانواده محترم که با حوصله خود مشغول من در انجام این کار بودند، تقدیر و تشکر می‌نماید و لازم می‌دانم از معاونت و مدیریت محترم پژوهشی دانشگاه و همکاران محترم آن حوزه به خاطر همه نوع رحمت و مساعدت‌ها در انجام ویی کبری امور مربوط به داوری کتاب صمیمانه قدردانی کنم.

در حاتمه، از رحمت بی دریغ آقای مهندس حسن قربانزاد و نیز آقای آرمان شمسی‌زاد که در اعمال تصحیح‌های علمی و کمک در تنظیم جداول و شکل‌ها قدرانی می‌نمایم.

ناصر زمانی، دانشگاه محقق اردبیلی

شهریور ۱۳۹۳

zamani@iaia.ir

nasir.zamani@iaia.ac.ir