به نام خدا

دانشکده علوم، گروه ریاضی

پایان نامه کارشناسی ارشد

ریاضی کاربردی – تحقیق در عملیات

موضوع:

کدبرداری از کدهای خطی دودویی با استفاده از برنامه‌ریزی خطی

استاد راهنما:
دکتر محمد رضا پیغامی

استاد مشاور:
دکتر محمود هادی زاده

گرد آورنده:
محمد صادق برزگر

پاییز ۱۳۸۹

اظهارنامه دانشجو

موضوع پا یان نامه: کدبرداری از کدهای خطی دودویی با استفاده از برنامه‌ریزی خطی.

استاد راهنما: آقای دکتر محمد رضا پیغامی.

نام دانشجو: محمد صادق برزگر.

شماره دانشجویی: ۸۷۰۵۴۳۴

اینجانب محمد صادق برزگر ، دانشجوی کارشناسی ارشد رشته‌ی ریاضی کاربردی گرایش تحقیق در عملیات دانشکده علوم دانشگاه صنعتی خواجه نصیرالدین طوسی ، گواهی می‌نمایم که تحقیقات ارائه شده در این پایان‌نامه توسط شخص اینجانب انجام شده و صحت و اصالت مطالب نگارش شده مورد تأیید می‌باشد و در مورد استفاده از کار دیگر محققان به مرجع مورد استفاده اشاره شده است. هم چنین ، گواهی می‌نمایم که مطالب مندرج در پایان‌نامه تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگری در هیچ جا ارائه نشده است و در تدوین متن پایان‌نامه آئین نامه‌ی مصوب دانشگاه را به طور کامل رعایت کرده‌ام.

امضاء دانشجو:

تاریخ:

فرم حق طبع و نشر و مالکیت نتایج

۱—حق چاپ و تکثیر این پایان‌نامه متعلق به نویسنده آن می‌باشد . هرگونه کپی برداری به صورت کل پایان‌نامه یا بخشی از آن تنها با موافقت نویسنده یا کتابخانه دانشکده علوم پایه دانشگاه صنعتی خواجه نصیرالدین طوسی مجاز می‌باشد.

۲—کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی خواجه نصیرالدین طوسی می‌باشد و بدون اجازه کتبی دانشگاه به شخص ثالث قابل واگذاری نیست.

هم چنین ، استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

تشکر و قدردانی

شکر خداوند متعال را به جای آورده که توفیق نصیبم کرد تا این پایان‌نامه را به پایان برسانم. نگارنده بر خود فرض می‌داند که از زحمات بی‌دریغ ، تلاش‌های بی‌وقفه و راهنمایی‌های ارزشمند استاد گرامی جناب آقای دکتر محمد رضا پیغامی در راستای انجام این پروژه در طول این مدت تشکر و قدردانی نماید. از جناب آقای دکتر کسری علیشاهی (داور خارجی) ، دکتر فریده قریشی (داور داخلی) و دکتر محمود هادی زاده (استاد مشاور) ، نیز به جهت خواندن این پایان نامه و پیشنهادات ارزنده‌شان تشکر می‌کنم.

در پایان از کلیه کسانی که در طول دوره‌ی کارشناسی ارشد و نیز دوره‌ی کارشناسی راهنمای علمی اینجانب بوده‌اند و مرا در این راه یاری کرده‌اند صمیمانه تشکر می‌نمایم ، به خصوص از پدر و مادر مهربانم که در جهت تحصیل اینجانب از هیچ کوششی دریغ نورزیدند و همواره مشوق من بودند تشکر و قدردانی می‌نمایم و امیدوارم با تقدیم این پایان نامه به آنها توانسته باشم قدم دیگری در جهت پاسخ به زحمات بی‌شمارشان برداشته باشم.

فهرست مندرجات

چکیده ۹

پیش گفتار ۱۰

۱ مفاهیم و تعاریف اولیه ۱۵

۱.۱ برنامه‌ریزی خطی ۱۶

۲.۱ کانال‌های مخابراتی ۱۷
۱.۲.۱ کانال‌های مخابراتی گسسته ۱۹
۲.۲.۱ کانال با نویز سفید گوسی جمع شونده ۲۱

۳.۱ انواع کدها ۲۱
۱.۳.۱ کدهای قالبی خطی ۲۱
۲.۳.۱ نمایش ماتریسی کدهای قالبی خطی ۲۲
۳.۳.۱ کدهای چرخشی باینری ۲۵
۴.۳.۱ کدهای کانولوشن ۲۵
۵.۳.۱ کدهای توربو ۲۶
۶.۳.۱ کدهای بررسی درستی با چگالی کم $LDPC$ ۲۶
۷.۳.۱ گراف عامل ۲۷

۴.۱ فرضیات کانال ۲۹

۵.۱ کدبرداری از کدهای $LDPC$ ۳۰
۱.۵.۱ الگوریتم جمع–ضرب ۳۱
۲.۵.۱ الگوریتم معکوس کردن وضعیت بیت ۳۱

٦.۱ کدبرداری ML ۳۳

۲ روش برنامه‌ریزی خطی برای کدبرداری از کدهای $LDPC$ و تحلیل آن ۳۴

۱.۲ چند وجهی کلمه کد ۳۵

۲.۲ آزاد سازی LP ۳٦

۳.۲ حل LP و نمایش‌های چند وجهی ۴۰
۱.۳.۲ هم ارزی چند وجهی ۴۱
۲.۳.۲ چند وجهی تصویر شده ۴۲
۳.۳.۲ چند وجهی کد با چگالی بالا ۴۷

۴.۲ الگوریتم کدبرداری برنامه‌ریزی خطی چند گامی MLP ۵۱
۱.۴.۲ الگوریتم کدبرداری MLP ۵۱
۲.۴.۲ معیاری برای اضافه کردن قیود جدید ۵۴
۳.۴.۲ شبیه سازی نتایج و تحلیل آن ۵۵

۵.۲ جواب بهین چندگانه در کدبرداری برنامه‌ریزی خطی در کانال BSC ۵٦

٦.۲ راهکارهایی برای بهبود کدبرداری برنامه‌ریزی خطی ۵٦

۱.۶.۲ اضافه نمودن معادلات بررسی دیگر ۵۶
۲.۶.۲ بهینه کردن طراحی کد به کمک مسأله‌ی کمر گراف ۵۷
۳.۶.۲ بهینه کردن طراحی کد با طراحی زوج توزیع درجه مناسب ۵۸

۷.۲ شرایط موفقیت کدبردار LP ۶۰
۱.۷.۲ فرض تمام صفر (صفر کامل) ۶۱

۸.۲ مزایا و معایب کدبرداری برنامه‌ریزی خطی ۶۷
۱.۸.۲ خاصیت تأیید ML ۶۷
۲.۸.۲ حذف پارامتر سیگنال به نویز در فرایند کدبرداری ۶۷
۳.۸.۲ برخی معایب کدبرداری برنامه‌ریزی خطی ۶۸

۳ شبه کلمه کدها و فاصله‌ی کسری ۶۹

۱.۳ شبه کلمه کد ۷۰
۱.۱.۳ گراف(های) شبه کلمه کد ۷۳

۲.۳ فاصله‌ی کسری ۷۶
۱.۲.۳ تعاریف و خواص پایه‌ای ۷۶
۲.۲.۳ محاسبه‌ی فاصله‌ی کسری ۷۸
۳.۲.۳ تجربه عملی ۷۹
۴.۲.۳ فاصله‌ی کسری ماکزیمم ۸۱
۵.۲.۳ یک کران پایین با استفاده از کمر ۸۲

۴ مقایسه کدبردار LP با دیگر کدبردارها ۸۷

۱.۴ مجموعه‌ی توقف در کانال بی‌حافظه‌ی دودویی ۸۸

۲.۴ کدهای دوری ۹۰

۳.۴ شبکه‌های دنباله—تیز ۹۱

۴.۴ درخت دوباره وزن دهی شده ماکزیمم—ضرب ۹۲

۵.۴ کدبرداری مینیمم—جمع ۹۲
۱.۵.۴ درخت محاسبات ۹۴

۶.۴ الگوریتم تکراری جدید و خاصیت تأیید ML از دوگان LP ۹۵
۱.۶.۴ مقایسه‌ی عملی ۹۶

۷.۴ آزاد سازی تنگ‌تر ۹۷

۸.۴ کدبرداری ML با استفاده از برنامه‌ریزی عدد صحیح ۹۹

نتیجه گیری و پیشنهاد برای کارهای آتی ۱۰۱

کتاب نامه ۱۰۲

چکیده

در این پایان نامه ، روشی برای تقریب حداکثر احتمال (ML) کدبرداری از یک کد خطی دودویی دلخواه ارائه می‌گردد که مبتنی بر مشاهدات دریافتی از یک کانال متقارن بی حافظه‌ی گسسته می‌باشد. الگوریتم کدبرداری بر اساس یک آزاد سازی برنامه‌ریزی خطی (LP) است که توسط یک گراف عامل یا یک نمایش بررسی درستی از یک کد تعریف می‌شود.
یک توصیف ترکیبیاتی دقیق از زمانی که یک کدبردار موفق عمل می کند بر مبنای شبه کلمات کد متناظر با گراف عامل ارائه می‌شود. هم چنین ، تعریف شبه کلمه کد برای روش‌های تکراری منجر به یکسان سازی نمادها از قبیل مجموعه‌ی توقف ، گردش بسته‌ی تحویل ناپذیر ، دورهای شبکه‌ای ، مجموعه‌های انحراف و پوشش گراف خواهد شد.

فاصله‌ی کسری d_{frac} برای یک کد تعریف می‌شود که یک کران پایین برای فاصله‌ی کلاسیک است. در ادامه نشان می‌دهیم کدبردار LP دامنه‌ی خطا را تا $\lceil d_{frac}/2 \rceil - 1$ تصحیح می‌کند. هم چنین ، کدهایی با $d_{frac} = \Omega(n^{1-\epsilon})$ وجود دارند و یک الگوریتم مؤثر برای محاسبه‌ی فاصله‌ی کسری ارائه می‌کنیم. نتایج تجربی عملکرد مشابهی را بر کدهای بررسی درستی با چگالی کم $(LDPC)$ در بین روش‌های کدبردار LP ، مینیمم–ماکزیمم و الگوریتم جمع–ضرب نشان می‌دهد ، به همین منظور روش‌هایی برای تنگ‌تر کردن آزاد سازی LP برای بهبود عملکرد ارائه می‌گردد.

اصطلاحات :

انتشار باور ، کدبرداری تکراری ، کد بررسی درستی با چگالی کم $(LDPC)$ ، کدهای خطی ، برنامه‌ریزی خطی LP ، آزاد سازی برنامه ریزی خطی ، کانال مخابراتی ، مجموعه‌ی توقف ، کمترین فاصله ، شبه کلمه کد.

پیش گفتار

فرض کنید در یک ارتباط دیجیتال با یک کانال مخابراتی نویزدار روبرو هستیم ، که هدف این کانال ارسال اطلاعات مطمئن در مسیر کانال مخابراتی می‌باشد. شانون[۱] در [۱۳] نشان داد که انتقال مطمئن اطلاعات بر روی کانال زمانی امکان پذیر است که نرخ اطلاعات[۲] در کانال کمتر از ظرفیت کانال[۳] باشد. برای رسیدن به حد شانون احتیاج به استفاده از الگوریتم‌های کدگذاری قوی می‌باشد. در چند سال اخیر با توجه به کشف مجدد کدهای بررسی درستی با چگالی کم[۴] $(LDPC)$ تقریباً بهترین کدهای عملیاتی برای رسیدن به ظرفیت کانال شناسایی شده است.

کدهای بررسی درستی با چگالی کم برای اولین بار توسط گالاگر[۵] [۸] در سال ۱۹۶۲ کشف شد و در دهه‌ی نود توسط تعدادی از محققین بازیابی شد که تا کنون مورد توجه قرار گرفته است [۹]،[۵]، [۱۱]. ولی عمل تصحیح خطای این نمونه از کدها پیشرفت زیادی حاصل نکرده است. در واقع ، چانگ[۶] در [۱۲] خانواده‌ای از کدهای $LDPC$ را معرفی کرده که در dB ۰/۰۰۴۵ از ظرفیت کانال اتفاق می‌افتد.

اغلب کدبردارهای مورد استفاده برای کدبرداری این خانواده از کدها بر اساس الگوریتم انتشار باور[۷] (BP) [۱۴] برنامه‌ریزی شده‌اند که پیام‌ها به طور متناوب در جهت گراف عامل ساختار کد فرستاده می‌شوند. در حالی که این کدبردار کاملاً خوب عمل می‌کند بررسی رفتار آن زمانی که گراف عامل[۸] دارای دور باشد اغلب دشوار است.

در این پایان نامه الگوریتمی برای یک کد خطی دودویی دلخواه بر مبنای یک آزاد سازی برنامه‌ریزی خطی[۹] (LP) معرفی می‌کنیم. برای این منظور ، یک چند وجهی ، که شامل کلیه‌ی کلمه کدهای ممکن است ، طراحی کرده و یک تابع هدف که کلمه کد با حداکثر احتمال[۱۰] (ML) نقطه‌ی بهینه‌ی آن با مؤلفه‌های صحیح است در نظر می‌گیریم. برنامه‌ریزی خطی را برای یافتن نقطه بهینه‌ی (احتمالاً کسری) چند وجهی به کار می‌بریم و زمانی به موفقیت می‌رسیم که آن نقطه‌ی بهینه کلمه کد انتقال یافته باشد. آزمایش‌های

---

[۱] Shannon
[۲] Information Rate
[۳] Channel Capacity
[۴] Low-Density Parity Check
[۵] Gallagar
[۶] Chung
[۷] Belief-Propagation Algorithm
[۸] Factor Graph
[۹] Linear Programing
[۱۰] Maximum-Likelihood

انجام شده بر کدهای $LDPC$ نشان می‌دهد نتایج کدبردار LP بهتر از الگوریتم مینیمم—جمع است. به علاوه ، کدبردار LP دارای خاصیت تأیید ML است یعنی ، « هرگاه خروجی کدبردار LP یک کلمه کد باشد تضمین می‌کند که کلمه کد ML است ». هیچ یک از روش‌های تکراری استاندارد این خصوصیت مطلوب را ندارند.

یک ویژگی خوب کدبردار LP احساس مسئولیت آن در قبال آنالیز شدن است. در این پایان نامه ، روش‌های متنوعی جهت آنالیز عملکرد این روش معرفی خواهد شد. هم چنین ، یک توصیف ترکیبیاتی دقیق از قیود برای موفقیت کدبردار LP ، حتی با وجود دور در گراف عامل ، ارائه می‌کنیم. این توصیف برای هر کانال متقارن بی‌حافظه‌ی گسسته[۱۱] نیز برقرار خواهد بود ؛ در چنین کانال‌هایی تابع هزینه خطی می‌تواند بر بیت‌های کد طوری تعریف شود که کلمه کد با کمترین هزینه ، کلمه کد ML باشد. در ادامه ، مجموعه شبه کلمه کدها[۱۲] را معرفی می‌کنیم که یک مجموعه‌ی بالایی از مجموعه کلمه کدهاست. نشان می‌دهیم که کدبردار LP همیشه شبه کلمه کد با کمترین هزینه را خواهد یافت. بنابراین ، کدبردار LP موفق است اگر و تنها اگر کلمه کد با کمترین هزینه همان کلمه کد ارسال شده باشد.

هم چنین در این پایان نامه ، مفهوم فاصله‌ی کسری[۱۳] d_{frac} از یک گراف عامل را تعریف می‌کنیم که کمترین فاصله بین کلمه کد و شبه کلمه کد را بیان می‌کند. به دلیل تضمینی که برای عملکرد دقیق کدبردار ML روی فاصله‌ی کلاسیک[۱۴] وجود دارد ، ثابت خواهیم کرد که کدبردار LP می‌تواند حداکثر $۱ - [\frac{d_{frac}}{۲}]$ خطا را در کانال متقارن دودویی (BSC)[۱۵] تصحیح نماید. هم چنین ، ثابت خواهیم کرد که فاصله‌ی کسری کد خطی با گره بررسی از درجه حداقل سه ، نسبت به کمر[۱۶] گراف مرتبط با کد حداقل نمایی می‌باشد. بنابراین ، در یک گراف با کمر لگاریتمی فاصله‌ی کسری از پایین کرندار به $\Omega(n^{۱-\epsilon})$ ، برای ثابت ϵ ، می‌باشد که در آن n طول کد است.
در کدهای $LDPC$ ثابت می‌شود که فاصله‌ی کسری به طور مؤثر قابل محاسبه است. این کمیت نه تنها برای ارزیابی عملکرد کد تحت کدبردار LP مفید است ، بلکه به عنوان کران پایینی در فاصله‌ی حقیقی[۱۷] کد می‌تواند مورد استفاده قرار گیرد.

---

[۱۱] Discrete Memoryless Symmetric Channel
[۱۲] Pseudocodeword
[۱۳] Fractional Distance
[۱۴] Classical Distance
[۱۵] Binary-Symmetric Channel
[۱۶] girth—طول کوتاهترین دور در گراف تنر را کمر گویند.
[۱۷] True Distance

ارتباط با الگوریتم‌های تکراری

روش‌هایی که توسط چانگ در [۱۲] برای تحلیل کدهای $LDPC$ مورد استفاده قرار گرفت بر اساس کار اربانک[۱۸] و ریچاردسون[۱۹] در [۱۵] و لابی[۲۰] و همکارانش در [۱۶] بود که الگوریتمی را برای محاسبه‌ی آستانه‌ی کدهای $LDPC$ با ساختار تصادفی ارائه کردند. این آستانه[۲۱] به عنوان حد نویز کانال عمل می‌کند ؛ اگر نویز کمتر از حد یا آستانه باشد ، در صورتی که طول بلوک به بینهایت میل کند ، آنگاه با استفاده از الگوریتم انتشار باور می‌توان به یک کدبردار قابل اعتماد رسید.
تحلیل آستانه بر مبنای ایده‌ی در نظر گرفتن یک دسته از کدها جهت آنالیز آنهاست. در واقع ، میانگین این دسته وقتی طول کد به بینهایت میل می‌کند ، به عنوان رفتار کد در نظر گرفته می‌شود. برای ثابت ϵ ، برای بسیاری از دسته‌ها در [۱۰] ثابت شده است که اختلاف در نرخ خطا[۲۲] (تحت کدبردار BP) بین یک کد تصادفی[۲۳] و کد میانگین[۲۴] در آن دسته ، در طول بلوک با احتمال به طور نمایی کوچک کمتر از ϵ می‌باشد.

محاسبه‌ی نرخ خطای میانگین دسته ، زمانی که گراف عامل شامل دور باشد می‌تواند مشکل باشد ، زیرا الگوریتم‌های تکراری می‌توانند دورها را مکرراً طی کنند. هم چنین ، نویز در کانال می‌تواند به طرز پیچیده‌ای در تصمیم نهایی مؤثر باشد. با در نظر گرفتن حالت حدی برای طول بلوک بینهایت می‌توان این پیچیدگی را نادیده گرفت. در این صورت ، احتمال این که یک پیام بارها یک دور را بپیماید به صفر همگرا خواهد شد. با این وجود ، در بسیاری از طول کدهای عملی ، این ایده به سمت یک تقریب ضعیف از نرخ خطای واقعی [۱۰] می‌انجامد.
بنابراین ، بررسی رفتار یک دسته از کدها با طول بلوک ثابت جهت درک تأثیر دورها بسیار ارزشمند خواهد بود. دای[۲۵] و همکاران در [۱۰] تحت کانال بی‌حافظه‌ی دودویی[۲۶] (BEC) تحلیلی از کدهای $LDPC$ با طول متناهی ارائه کرده‌اند. نکته کلیدی در نتایج آنها توجه به ساختار ترکیبیاتی محض مسأله است که به

---

[۱۸] Urbank
[۱۹] Richardson
[۲۰] Luby
[۲۱] Threshold
[۲۲] error rate
[۲۳] Random Code
[۲۴] Average Code
[۲۵] Di
[۲۶] Binary Erasure Channel

عنوان مجموعه‌ی توقف[۲۷] شناخته می‌شود. در حقیقت ، کدبردار BP شکست می‌خورد اگر و تنها اگر یک مجموعه‌ی توقف در میان بیت‌های پاک شده موجود باشد. بنابراین ، نرخ خطای BP به مفهوم ترکیبیاتی خالص کاهش می‌یابد.
برای کانال‌های BEC ثابت می‌کنیم که شبه کلمه کدها همان مجموعه‌ی توقف هستند و در نتیجه عملکرد کدبردار LP مشابه عملکرد کدبردار BP در کانال BEC است. مفهوم شبه کلمه کد که در اینجا بیان می‌شود با برخی نتایج شناخته شده برای حالت‌های خاص از کدها و کانال هماهنگ است. به عنوان مثال در شبکه‌های دنباله—تیز[۲۸] ، شبه کلمه کدهای معادل ، همان تعریف ارائه شده توسط فورنی[۲۹] در [٦] می‌باشد. هم چنین ، شبه کلمه کدها زمانی که برای تحلیل درخت‌های محاسبه برای کدبردار مینیمم—جمع به کار می‌روند با مجموعه‌های انحراف ، تعریف شده توسط وایبرگ[۳۰] در [۵] و تصحیح شده توسط فورنی در [۷] و فری[۳۱] ، کوتر[۳۲] و واردی[۳۳] در [۱۷] ، ارتباط دارند.

نتایج گذشته

در مراجع [۲] و [۳] فلدمن و همکاران روش کدبرداری از هر کد شبه توربو [۳۴] را بر اساس جریان شبکه‌ای مشابه[۳۵] و روش آزاد سازی برنامه‌ریزی خطی [۳٦] معرفی کردند. یک توصیف ترکیبیاتی دقیق از شرایطی که تحت آن این کدبردار موفق است ارائه می‌شود. از ویژگی‌های کدبردار LP استفاده کرده و یک کد از رده کدهای توربوی ساده به نام تکرار—انباشتگی[۳۷] (RA) با نرخ ۱/۲ طراحی شده است. یک کران بالا برای احتمال خطای کدبردار به دست آورده و نحوه‌ی طراحی الگوریتم‌های تکراری بیشتر برای داشتن عملکردی همانند عملکرد کدبردار LP را توضیح می‌دهیم.

---

[۲۷] Stopping Set
[۲۸] Tail-Biting Trellises
[۲۹] Forney
[۳۰] Wiberg
[۳۱] Frey
[۳۲] Koetter
[۳۳] Vardy
[۳۴] Turbo-Like
[۳۵] Similar Network Flow
[۳٦] Linear Programming Relaxation
[۳۷] Repeat-Accumulate

طرح کلی

این پایان نامه در چهار فصل تنظیم شده است. در فصل اول سعی بر آن شده تا جایی که مجال است مفاهیم و تعاریف اولیه‌ی مورد نیاز برای درک بهتر مطالب پایان نامه ذکر شود. از این رو خلاصه‌ای از برنامه‌ریزی خطی ، انواع کانال‌ها و کدهای مخابراتی از جمله کانال مخابراتی گسسته و کدهای بررسی درستی با چگالی کم به همراه گراف عامل کد بیان شده است. کدهای دیگری هم برای تجربه‌ی عملی و مقایسه بین چند نمونه کد تشریح شده است. در ابتدای فصل دوم چند وجهی کلمه کد معرفی می شود که این چند وجهی دقیقاً همان ناحیه‌ای است که بهینه سازی برنامه‌ریزی خطی برای به دست آوردن کلمه کد ارسال شده در طول کانال مخابراتی روی آن انجام می‌پذیرد. به منظور کاهش حجم عملیات کدبرداری به روش برنامه‌ریزی خطی چند وجهی‌های متعدد دیگری معرفی می‌شوند که همگی معادل یکدیگرند. سپس ، حالات مختلفی که ممکن است در حین اجرای عملیات کدبرداری LP پیش آید مورد بررسی قرار می گیرد و راهکارهایی برای رفع نقایص آن پیشنهاد خواهد شد. در ادامه به تحلیل کدبرداری LP پرداخته‌ایم و خواهیم دید که می‌توان برای ساده‌تر کردن شرایط تحلیل فرض کرد که کلمه کد ارسال شده در طول کانال مخابراتی یک کد تمام صفر است.

فصل سوم از این پایان نامه اختصاص به معرفی شبه کلمه کدها و فاصله‌ی کسری دارد. آنچه که در این فصل از اهمیت بیشتری برخوردار است تجربه‌ی عملی کدبردار LP و مقایسه‌ی بین کدها و کانال‌های مختلف است. در فصل چهار که فصل نهایی این پایان نامه نیز هست تلاش می‌شود تا کدبرداری LP با دیگر کدبردارهای موجود مقایسه شود و روش‌هایی نیز برای بهبود عملکرد کدبرداری LP ارائه شود و به درستی که این فصل بیانگر دلیل تمام تلاش‌های کارشناسان برای معرفی کدبرداری برنامه‌ریزی خطی جهت کدبرداری از کدهای مخابراتی است.

فصل ۱

مفاهیم و تعاریف اولیه

این فصل اختصاص به معرفی و تعریف برخی مفاهیم مورد استفاده در این پایان نامه دارد. تعدادی از تعاریف که نیازی به پیش دانسته‌ها ندارند به طور مستقیم و کامل ارائه شده است. از آنجا که برخی از مفاهیم برای تفهیم به خواننده نیاز به پیش زمینه‌هایی دارند ، در این فصل تنها اشاره‌ای به صورت کلی آنها شده و توضیحات مکمل در فصل‌های آتی بیان خواهد شد. ابتدا به معرفی کانال‌های مخابراتی مورد استفاده در این پایان نامه ، از جمله کانال گسسته متقارن دودویی و کانال بی‌حافظه دودویی ، به همراه برخی ویژگی‌های مهم آنها خواهیم پرداخت. در ادامه ، کدها و به ویژه کدهای بررسی درستی با چگالی کم را شرح خواهیم داد که اساس کدبرداری در این پایان نامه بر این کدها استوار خواهد بود. سپس ، مفاهیم مرتبط با کدهای $LDPC$ از جمله گراف عامل را بیان می‌کنیم. هم چنین ، در انتها چند الگوریتم کدبرداری و خواص مربوط به آنها به طور خلاصه ذکر شده است. اکثر مطالب ذکر شده در این فصل از مراجع [۱] ، [۸] ، [۲۷] ، [۲۸] و [۳۵] انتخاب شده است.

۱.۱ برنامه‌ریزی خطی

یک مسأله‌ی برنامه‌ریزی ریاضی که در آن تابع هدف و محدودیت‌ها بر حسب متغیرها ، همگی خطی بوده و هیچ گونه شرط صحیح بودن روی متغیرهای تصمیم وجود ندارد ، برنامه‌ریزی خطی[۱] نامیده می‌شود. یک مسأله‌ی برنامه‌ریزی خطی دارای دو فرم اصلی متعارفی و استاندارد می‌باشد.
در فرم متعارفی، شکل کلی مسأله‌ی مینیمم سازی به صورت زیر است :

$$\begin{aligned} \min \quad & c^T x \\ s.t \quad & Ax \geq b \\ & x \geq 0 \end{aligned}$$

که در آن $A \in \mathbb{R}^{m \times n}$ ، $c, x \in \mathbb{R}^n$ و $b \in \mathbb{R}^m$ می‌باشند. به علاوه، b_i ها می‌توانند مثبت یا منفی باشند.
فرم استاندارد یک مسأله‌ی برنامه‌ریزی خطی در حالت مینیمم سازی به صورت زیر است :

$$\begin{aligned} (LP) \qquad \min \quad & c^T x \\ s.t \quad & Ax = b \\ & x \geq 0 \end{aligned}$$

[۱] Linear Programming

لازم به ذکر است که در این فرم برنامه‌ریزی ، بردار سمت راست b ، بایستی نامنفی باشد. در هر دو فرم فوق شرط نامنفی بودن $x \geq 0$ به مفهوم نامنفی بودن کلیه‌ی درایه‌های x می‌باشد.
نکته‌ی قابل توجه این است که هر مسأله‌ی برنامه‌ریزی خطی را می‌توان به کمک متغیرهای کمبود و مازاد به فرم استاندارد تبدیل کرد.

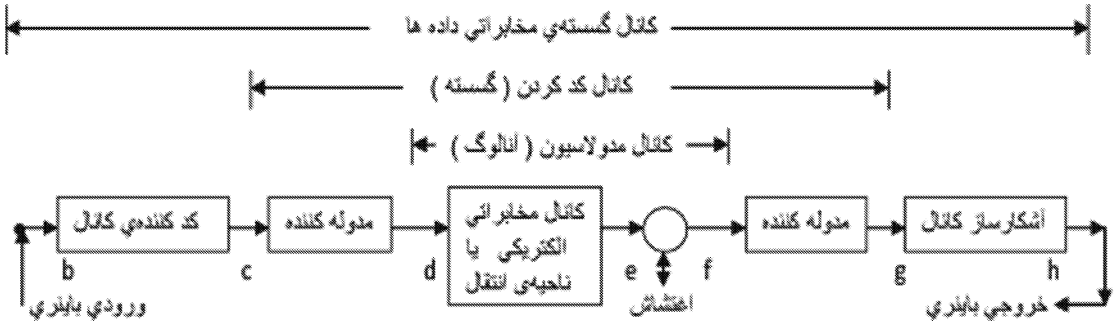
۲.۱ کانال‌های مخابراتی

یک سیستم مخابراتی را می‌توان به قسمت‌های فرستنده ، کانال فیزیکی یا محیط انتقال و گیرنده تقسیم نمود. فرستنده شامل یک کد کننده و یک مدوله کننده است ، در صورتی که گیرنده شامل یک دمدوله کننده و یک آشکار ساز می‌باشد. کانال‌های مخابراتی برحسب نقاط انتهایی و عملکرد ، معانی و خصوصیات متفاوتی می‌سازند.

بین نقاط c و g در شکل ۱ ، یک کانال گسسته که غالباً کد کننده نامیده می‌شود موجود است که دنباله‌ای از سمبل‌ها را به عنوان ورودی پذیرفته و دنباله‌ای از سمبل‌ها را در خروجی خود تولید می‌کند. این کانال به طور کامل توسط احتمال انتقال p_{ij} (p_{ij} برابر است با احتمال اینکه خروجی کانال سمبل j—ام از الفبا باشد وقتی ورودی آن سمبل i—ام است) مشخص می‌شود. این احتمال‌ها به پارامترهای مدولاتور ، محیط انتقال، اغتشاش و آشکار ساز بستگی دارند.

کانال مخابراتی موجود بین نقاط d و f در سیستم ، ارتباط الکتریکی بین فرستنده و گیرنده را تأمین می‌کند. ورودی و خروجی آن به شکل موج‌های الکتریکی پیوسته (آنالوگ) هستند. این قسمت از کانال یک کانال پیوسته یا کانال مدوله کننده می‌باشد. این کانال‌ها در معرض خرابی‌های متنوعی مانند فرکانس کانال و عوامل غیر خطی در کانال می‌باشند. به علاوه ، کانال تحت تأثیر اغتشاش و تضعیف‌های تصادفی[۲] (تغییرات و تضعیف‌های تصادفی در محیط انتقال) می‌تواند باعث خرابی سیگنال ورودی شود. تمام این خرابی‌ها باعث داخل شدن خطا و در نتیجه محدود شدن میزان ماکزیمم برای انتقال اطلاعات توسط کانال خواهند شد.

---
[۲] Fades



شکل ۱ مدل یک کانال مخابراتی باینری

۱.۲.۱ کانال‌های مخابراتی گسسته

کانال مخابراتی بین نقاط c و g در شکل ۱ ، یک کانال گسسته است. در حالت کلی ، ورودی کانال سمبلی است که به الفبایی با M سمبل متعلق است. خروجی کانال نیز سمبلی است که به همان الفبای M سمبلی ورودی متعلق است. سمبل خروجی به خاطر خطاهای تحمیل شده در کانال ممکن است متفاوت از سمبل ورودی باشد. این خطاها اصولاً ناشی از اغتشاش در قسمت آنالوگ کانال مخابراتی می‌باشند. کانال گسسته به طور کامل توسط مجموعه احتمالات p_j^r برای $j = ۱, ۲, \ldots, M$ ، p_i^t برای $i = ۱, ۲, \ldots, M$ و p_{ij} برای $i, j = ۱, ۲, \ldots, M$ مدل سازی می‌شود. p_i^t احتمال انتخاب i—امین سمبل به عنوان ورودی کانال ، p_j^r احتمال دریافت سمبل j—ام و p_{ij} احتمال دریافت j—امین سمبل در خروجی کانال ، هنگامی که i—امین سمبل به عنوان ورودی کانال انتخاب شده است ، می‌باشند. کانال‌هایی که برای انتقال و دریافت یکی از M سمبل مختلف طراحی می‌شوند به کانال‌های M—تایی[۳] موسوم‌اند. مدل آماری یک کانال گسسته‌ی باینری در شکل دو نمایش داده شده است. ورودی این کانال متغیر تصادفی باینری X است و دو گره در سمت چپ گراف شکل دو بیانگر مقادیر صفر و یک متعلق به متغیر تصادفی X است. خروجی کانال نیز یک متغیر تصادفی باینری است (Y) که مقادیرش روی گره‌های سمت راست گراف نمایش داده شده است. چهار مسیر مختلف ، گره‌های ورودی را به گره‌های خروجی مرتبط می‌سازند. مسیر بالای گراف بیانگر ورودی صفر و خروجی غلط یک است. خطاها به سبک تصادفی اتفاق می‌افتند و وقوع خطاها را می‌توان با تخصیص احتمال به مسیرهای مختلف و به طور آماری مدل سازی نمود. فرض کنیم که وقوع خطا در هر فاصله‌ی زمانی ارسال یک بیت تأثیری روی رفتار سیستم در سایر زمان‌ها نداشته باشد (یعنی فرض کنیم که کانال

[۳] M-ary

بدون حافظه باشد). در این صورت با یک کانال گسسته‌ی بی‌حافظه (BEC) سروکار داریم. فرض کنید :

$$P(X=۰)=p_۰^t\ ,\ P(X=۱)=p_۱^t\ ,\ P(Y=۰)=p_۰^r\ ,\ P(Y=۱)=p_۱^r$$

در این صورت خواهیم داشت :

$$P(error)=P_e=P(X\neq Y)=P(X=۰,Y=۱)+P(X=۱,Y=۰)$$
$$=P(Y=۱|X=۰)P(X=۰)+P(Y=۰|X=۱)P(X=۱)$$

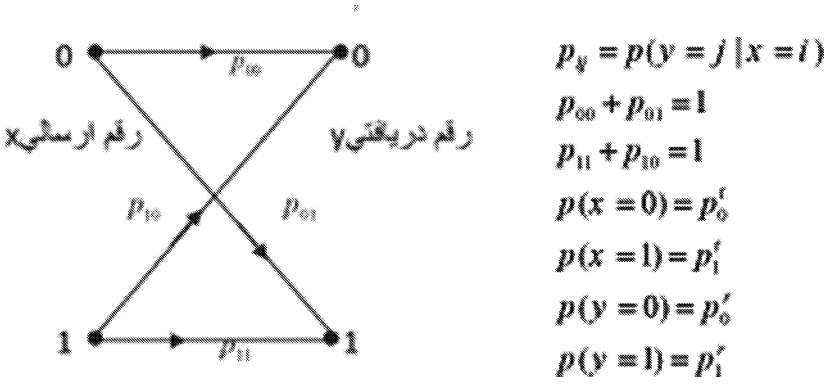
و یا

$$P_e\ =\ p_۰^t\ p_{۰۱}\ +\ p_۱^t\ p_{۱۰}$$

هم چنین ، $p_۰^r$ و $p_۱^r$ را می‌توان به صورت زیر بیان نمود :

$$p_۰^r\ =\ p_۰^t\ p_{۰۰}\ +\ p_۱^t\ p_{۱۰}$$
$$p_۱^r\ =\ p_۰^t\ p_{۰۱}\ +\ p_۱^t\ p_{۱۱}$$

در صورتی که $p_{۰۰}=p_{۱۱}=p$ باشد ، کانال را کانال باینری متقارن (BSC) گوییم. در این صورت برای بیان احتمالات کانال فقط به یک پارامتر p نیاز است.



شکل ۲ مدل یک کانال گسسته

۲.۲.۱ کانال با نویز سفید گوسی جمع شونده

مهمترین مدل کانال پیوسته کانال با نویز سفید گوسی جمع شونده[۴] ($AWGN$) است. این کانال می‌تواند روی پهنای باند ، انتقالی بدون اعوجاج ایجاد کند و تلفات انتقال با تقویت جبران می‌شود. برای اطلاعات بیشتر از ویژگی‌های این کانال به مرجع [۲۷] مراجعه نمایید.

۳.۱ انواع کدها

کدهای کنترل خطا غالباً به دو دسته‌ی وسیع تقسیم می‌شوند : کدهای بلوکی یا قالبی[۵] و کدهای کانولوشن[۶]. در کدهای قالبی ، یک قالب مرکب از k بیت اطلاعات ، توسط یک گروه مرکب از r بیت بررسی که از روی قالب بیت‌های اطلاعات به دست می آیند ، دنبال می‌شود. در گیرنده ، بیت‌های بررسی برای بررسی بیت‌های اطلاعات در قالب مقدم بر بیت‌های بررسی به کار برده می‌شوند. در کدهای کانولوشن ، بیت‌های بررسی به طور پیوسته لابه‌لای بیت‌های اطلاعاتی قرار می‌گیرند. بیت‌های بررسی نه فقط برای بررسی بیت‌های اطلاعات در قالب مقدم بر بیت‌های بررسی ، بلکه برای بررسی سایر قالب‌ها نیز به کار برده می‌شوند.

۱.۳.۱ کدهای قالبی خطی

در این بخش به معرفی مختصر کدهای قالبی می‌پردازیم که در آنها قالب‌های پیام k بیتی به یک قالب پیام $n > k$ بیتی ، مطابق شکل ۳ ، با افزودن $n-k$ بیت بررسی مناسب از روی k بیت پیام ، کد می‌شوند.

قالب n بیتی خروجی کد کننده‌ی کانال را کلمه کد[۷] گویند و کدهایی که در آنها بیت‌های پیام در آغاز کلمه کد قرار می‌گیرند به کدهای سیستماتیک[۸] معروفند. به علاوه ، اگر هر یک از ۲^k کلمه کد را بتوان به صورت ترکیب خطی از k بردار خطی مستقل بیان نمود ، در این صورت کد را کد قالبی خطی سیستماتیک نامند[۲۸].

---

[۴] Additive White Gaussian Channel
[۵] Block Codes
[۶] Convolutional Codes
[۷] Code Word
[۸] Systematic Codes