دانشگاه صنعتی شاهرود
دانشکده علوم ریاضی
گروه ریاضی

پایان‌نامه کارشناسی ارشد ریاضی

عنوان

بررسی کدهای خطی و غیر خطی و برخی کاربردهای آن(کدهایDPCL)

نگارش
مهناز علیین

استاد راهنما
آقای دکتر صادق رحیمی شعرباف

استاد مشاور
آقای دکتر جعفری‌راد

۱۳۹۰/۲/۱۳

صفحة تصويب نامه توسط هيأت داوران (فرم پيوست ۳ يا ۴ با امضاي اصل هيأت داوران مورد قبول است)

قدردانی

به نام یاربی همتا

من لم یشکر المخلوق لم یشکر الخالق

با سلام و درود به ارواح طیبه شهدا از صدر اسلام تا کنون و تهیت و ثنا بر یگانه منجی عالم بشریت حضرت ولی عصر (عج) روحی فداک و نائب بر حقش، بر خود دانستم تا مراتب تشکر و قدردانی خود را از کلیه اساتید که بنده حقیر را در این چند سال مورد عنایت و راهنمایی قرار دادند، بنمایم و خواستار صحت و توفیقات روزافزون ایشان و خانواده محترمشان از خداوند بی همتا باشم. امید آن دارم که این تلاش جزئی و ناچیز که تقدیم به مهدی فاطمه سلام ا... علیه نموده‌ام مورد رضایت قلبی ایشان قرار گیرد.

تقدیر، تقویم انسان‌های عادیست و تغییر، تدبیر انسان‌های عالی. لحظاتی سرشار از تغییرات زیبا را برای کلیه محققان و اساتید گرامی از خداوند منان خواستارم.

چکیده

استفاده از کدهای LDPC به دلیل ساختار ساده، روش‌های کدگشایی تکراری و برخی دلایل دیگر در سال‌های اخیر بسیار مورد توجه بوده است. در این پایان‌نامه با نگاهی کوتاه به تاریخچه نظریه کدگذاری و بیان خلاصه‌ای از مفاهیم مربوط به کدهای خطی به شرح کدهای LDPC و نحوه کدگذاری آنها می‌پردازیم. سپس با استفاده از تعریف گراف فاکتور، برخی از الگوریتم‌های کدگشایی عبورپیام را معرفی می‌کنیم. علاوه‌براین روش کدگشایی برنامه‌ریزی خطی و برخی از مهمترین بهبودهای انجام شده بروی این الگوریتم کدگشایی را مورد بررسی قرار می‌دهیم و در پایان به مقایسه چند الگوریتم کدگشایی با استفاده از نتایج برخی مقالات اخیر می‌پردازیم.

واژه‌های کلیدی: کدهای $LDPC$ ، گراف فاکتور ، گراف تنر ، الگوریتم عبور پیام ، گدگشایی ، کدگذاری، کدهای خطی ، برنامه‌ریزی خطی ، کدگشای LP .

پیشگفتار

با نگاهی به پیشرفت‌های روزافزون در زمینه ارتباطات ، نظریه اطلاعات و نظریه کدگذاری و با توجه به کاربرد وسیع مفاهیم موجود در ریاضیات محض و کاربردی در این رشته‌ها ، زمینه مناسبی برای انجام تحقیقات کاربردی با استفاده از مفاهیم ریاضی از جمله نظریه ترکیبیات و گراف در این حیطه وجود دارد. به عنوان مثال می‌توان به ارتباط بین طرح‌های ترکیبیاتی با کد و مفاهیمی مانند فاصله در نظریه کدگذاری و همچنین ساخت کدهایی با استفاده از ماتریس هادامار اشاره کرد. علاوه‌براین از برخی تعاریف و قضایای موجود در نظریه گراف می‌توان به نتایجی مشابه با برخی قضایا و نتایج ارئه شده در نظریه کدگذاری رسید. خواننده گرامی می‌تواند برای بررسی این نتایج به مراجع [۱۹]،[۱۶] ، [۱] و مراجعه کند. علاوه‌براین نظریه کدگذاری در بسیاری از علوم مورد استفاده قرار گرفته است که برخی از این کاربردها داخل متن ذکر شده است. یکی از کاربردهای جذاب نظریه کدگذاری در زمینه ژنتیک و کدگشایی DNA است [۲] . آنچه در این پایان‌نامه بیان می‌گردد بررسی کاربرد برخی تکنیک‌های ریاضی مانند استفاده از گراف دو بخشی ، برنامه‌ریزی خطی ، برش گوموری و برخی مفاهیم آماری در نظریه کدگذاری و به طور خاص در کدهای LDPC است [۴]،[۳].

فهرست مطالب

لیست تصاویر ر

۱ مقدمه و تاریخچه ۱

۱.۱ تاریخچه . . . ۱

۲.۱ سیستم ارتباطی . . . ۳

۳.۱ مدل‌های کانال مورد استفاده در این پایان‌نامه . . . ۵

۱.۳.۱ نسبت‌های درستنمایی . . . ۷

۴.۱ فرضیات . . . ۸

۵.۱ مقیاس گذاری LLR . . . ۹

۲ مروری بر کدهای خطی و برخی مفاهیم مورد نیاز ۱۱

۱.۲ مقدمه فصل . . . ۱۱

۲.۲ برخی تعاریف . . . ۱۱

۳.۲ کدهای بلوکی خطی . . . ۱۲

۴.۲ کدهای خطی هم‌ارز . . . ۱۴

۵.۲ کد هامینگ . . . ۱۶

۶.۲ کدگشایی . . . ۱۷

۳ کدهای LDPC ۲۰

۱.۳ مقدمه فصل . . . ۲۰

۲.۳ گراف فاکتور . . . ۲۱

۱.۲.۳ قانون توزیع پذیری و گراف فاکتور . . . ۲۱

۲.۲.۳ تعیین فرم بازگشتی توابع حاشیه‌ای . . . ۲۴

۳.۲.۳ حاشیه‌سازی از طریق عبور پیام . . . ۲۸

۴.۲.۳ کدگشایی MAPبیتی . . . ۳۰

۵.۲.۳ گراف‌های فاکتور سبک فورنی . . . ۳۲

۳.۳ کدهای بررسی‌زوجیت کم‌چگال (LDPC) . . . ۳۳

۱.۳.۳ انواع کدهای LDPC . . . ۳۴

۲.۳.۳ ساخت کدهای LDPC . . . ۳۸

۴.۳ کدگذاری . . . ۴۳

۱.۴.۳ کدگذاری پیچیدگی زمانی‌خطی ، برای کدهای LDPC ۴۵

۴ کدگشایی کدهای LDPC با استفاده از کدگشای عبورپیام ۵۳
۱.۴ مقدمه فصل ۵۳
۲.۴ عبور پیام تحت کانال پاک‌شدگی دودویی ۵۵
۳.۴ کدگشای معکوس کردن وضعیت بیت ۶۱
۴.۴ کدگشای جمع - ضرب ۶۷
۵.۴ تحلیل کدگشای عبور پیام (MPA) ۷۵
۱.۵.۴ تکامل چگالی روی BEC ۷۷
۲.۵.۴ آستانه ۸۳
۳.۵.۴ پایداری ۸۶
۴.۵.۴ کمر ۸۷
۵.۵.۴ کدواژه‌های کاذب ۸۹

۵ کدگشایی کدهای LDPC با استفاده از الگوریتم کدگشایی LP ۹۰
۱.۵ مقدمه فصل ۹۰
۲.۵ پیش نیاز ها ۹۱
۳.۵ فرمولبندی برنامه‌ریزی‌خطی کاهشی برای کدگشایی ۹۲
۱.۳.۵ کدگشایی ماکزیمم درستنمایی برای LP ۹۲
۲.۳.۵ بررسی جواب‌های کدگشای LP ۹۹
۳.۳.۵ مقیاس گذاری λ ۱۰۰
۴.۵ تفسیر هندسی ۱۰۱
۱.۴.۵ شرح چندسقفی $\mathcal{P}$ ۱۰۵
۵.۵ فرمول‌بندی جایگزینی ۱۰۸
۱.۵.۵ نکاتی درباره تفسیر هندس روش جایگزینی ۱۱۳
۶.۵ بهبود عملکرد کدگشای (LP) ۱۱۴
۱.۶.۵ بهبود عملکرد کدگشای LP با استفاده از محدودیت‌های افزونگی ۱۱۵
۷.۵ تحلیل کدگشای LP ۱۲۸
۱.۷.۵ فرض صفر ۱۲۹
۲.۷.۵ کدواژه‌های کاذب ۱۳۰
۳.۷.۵ فاصله کسری ۱۳۱

۶ نتایج عددی ۱۳۳
۱.۶ مقدمه فصل ۱۳۳
۲.۶ بررسی نتایج ۱۳۳

کتاب‌نامه ۱۳۸

واژه‌نامه فارسی به انگلیسی ۱۴۱

لیست تصاویر

۱.۱ برخی از رویدادهای مهم در کدگذاری ۲
۲.۱ سیستم ارتباطی ۳
۳.۱ BSCبا احتمال همگذری ϵ ۶
۴.۱ نمودار سمت راست BECبا احتمال پاکشدگی کانال δ و نمودار سمت چپ کانال (BI-AWGNC) نرمال شده است. ۶

۱.۳ گراف فاکتور متناظر با مثال ۲.۲.۳ درخت است. از دایره برای نمایش راس متغیر و از مربع برای نمایش راس کنترل استفاده می‌شود ۲۲
۲.۳ گراف فاکتور تابع عضویت مثال ۴.۲.۳ (گراف تنر) این گراف نیز درخت است ۲۴
۳.۳ فاکتور گیری کلی g و مثال ۵.۲.۳ . . . . . ۲۵
۴.۳ فاکتورگیری کلی g_k و مثال ۷.۲.۳ . . . . . ۲۷
۵.۳ حاشیه‌سازی تابع f از طریق عبور پیام. عبور پیام از راس‌های برگ آغاز می‌شود. پیام‌هایی که هر راس دریافت می‌کند پس از پردازش به راس والد خود می‌فرستد ۲۹
۶.۳ [۱۸] قوانین عبور پیام ۳۰
۷.۳ گراف فاکتور مساله کدگشایی MAPمثال (۱۰.۲.۳) ۳۱
۸.۳ [۱۸]شکل سمت راست گراف فاکتور سبک فورنی ، شکل سمت چپ گراف فاکتور ۳۲
۹.۳ [۱۸]شکل سمت راست گراف فاکتور سبک فورنی ، شکل سمت چپ گراف فاکتور ۳۳
۱۰.۳ [۱۸] فرم بالا مثلثی تقریبی H ۴۶

۱.۴ کدگشای عبور پیام بردار دریافتی $y = [0\ 0\ 1\ ?\ ?\ ?]^T$. هریک از شکل‌ها بیانگر تصمیمی است که الگوریتم براساس پیام‌های گام قبلی اتخاذ می‌کند. برای نمایش عبور پیام ۰ از یک یال ، آن یال با نقطه چین پر رنگ ، عبور پیام ۱ با خط و عبور پیام ? با نقطه چین کم رنگ نشان داده شده است ۶۰
۲.۴ کدگشای معکوس کردن وضعیت بیت برای بردار دریافتی $y = [1\ 0\ 1\ 0\ 1\ 1]^T$. هریک از شکل‌ها بیانگر تصمیمی است که الگوریتم براساس پیام‌های گام قبلی اتخاذ می‌کند. علامت $\times$ بیانگر این است که معادله بررسی‌زوجیت برقرار نیست و علامت $\surd$ بیانگر این است که معادله بررسی‌زوجیت برقرار است. برای نمایش عبورپیام صفر از یک یال ، آن یال را با نقطه چین و عبورپیام یک را با خط نشان می‌دهیم. ۶۴

۳.۴ کدگشای معکوس کردن وضعیت بیت برای بردار دریافتی $y = [۱\ ۰\ ۱\ ۰\ ۰\ ۱]$. هریک از شکل‌ها بیانگر تصمیمی است که الگوریتم براساس پیام‌های گام قبلی اتخاذ می‌کند. علامت $\times$ بیانگر این است که معادله بررسی‌زوجیت برقرار نیست و علامت $\surd$ بیانگر این است که معادله بررسی‌زوجیت برقرار است. برای نمایش عبور پیام صفر از یک یال ، آن یال را با نقطه چین و عبور پیام یک را با خط نشان می‌دهیم. ۶۶
۴.۴ مجموعه $S = \{۱, ۲, ۳\}$ نشان‌دهنده مجموعه توقف $[۷, ۴, ۳]$ - کدهمینگ ۷۶
۵.۴ احتمالات پاک‌شدگی محاسبه شده در مثال (۳.۵.۴) ۸۰
۶.۴ احتمالات پاک‌شدگی محاسبه شده در مثال (۴.۵.۴) ۸۱
۷.۴ احتمالات پاک‌شدگی محاسبه شده در مثال (۵.۵.۴) ۸۴
۸.۴ احتمالات پاک‌شدگی محاسبه شده در مثال (۵.۵.۴) (بررسی دوباره) ۸۵
۹.۴ نرخ خطای بیتی اجرای کدگشای جمع - ضرب تحت کانال AWGNبا استفاده از ماتریس بررسی‌زوجیت مثال (۶.۵.۴) ۸۸

۱.۵ شکل سمت چپ مکعب واحد و شکل سمت راست پوسته محدب (چندسقفی محلی) $r(۱)$. ۱۰۴
۲.۵ چند سقفی کدواژه‌های محلی ۱۰۵
۳.۵ [۲۵]رابطه بین چندسقفی $\mathcal{P}$ ، $conv(\mathcal{C})$ ، کدواژه‌ها، جواب های کسری و بردارλ ۱۰۶
۴.۵ ۴ نیم‌فضا ۱۰۹
۵.۵ نیم‌فضای حاصل از $(hs۲)$ ۱۱۰
۶.۵ گراف فاکتور (۷.۴.۳) کد هامینگ . راس‌هایی که با دایره نمایش داده می‌شوند ، راس متغیر و راس‌هایی که با مربع نمایش داده می‌شوند، راس‌های بررسی هستند. ۱۱۴
۷.۵ گراف فاکتور جدید ۱۱۸
۸.۵ شرح مثال ۳.۶.۵ . . . . . ۱۲۰

۱.۶ [۲۳]اجرای برخی الگوریتم‌های کدگشایی برای (۳،۴) - کد LDPCبا طول بلوکی ۱۰۰ . . . ۱۳۴
۲.۶ [۲۳] اجرای برخی الگوریتم‌های کدگشایی برای (۳،۴)- کد LDPC. با طول بلوکی ۲۰۰ . . ۱۳۵
۳.۶ [۲۳] اجرای برخی الگوریتم‌های کدگشایی برای (۱۵۵،۶۴)- کد LDPCتنر. ۱۳۶

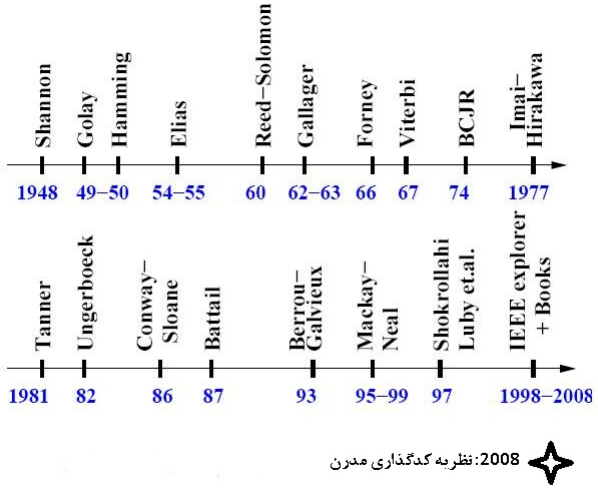
فصل ۱
مقدمه و تاریخچه

مساله اساسی ارتباطات تولید دوباره یک پیام (که در یک نقطه انتخاب شده است) در نقطه‌ای دیگراست. (کلود شانون) [۱]

۱.۱ تاریخچه

شانون در سال ۱۹۴۸ [۲۰] ، قوانینی را براساس ریاضیات بدست آورد که معین می‌کردند ، چگونه اطلاعات می‌توانند به سرعت از طریق یک کانال پارازیت‌دار ارسال شوند. مطالبی که شانون در این مقاله بیان می‌کند و چارچوب ریاضی آن ، مبنای تولید یک رشته کاملا جدید به نام **نظریه اطلاعات** [۲] گردید. تقریبا همزمان با شانون، **ریچارد هامینگ**[۳] (۱۹۵۰) به تحقیق درباره امکان کشف و تصحیح خطا در پیام‌های دریافتی پرداخته است. به این ترتیب با کار این دو (براساس چارچوب مطرح شده توسط شانون) [۴] نظریه کدگذاری یا به طور دقیق‌تر **نظریه کدهای تصحیح کننده خطا** [۵] شروع به کار کرد. می‌توان این گونه برداشت کرد که در حقیقت شانون نظریه کدگذاری را به دو قسمت **نظریه کدگذاری منبع** [۶] و **نظریه کدگذاری کانال** [۷] (کدهای تصحیح کننده خطا) تقسیم کرده است.

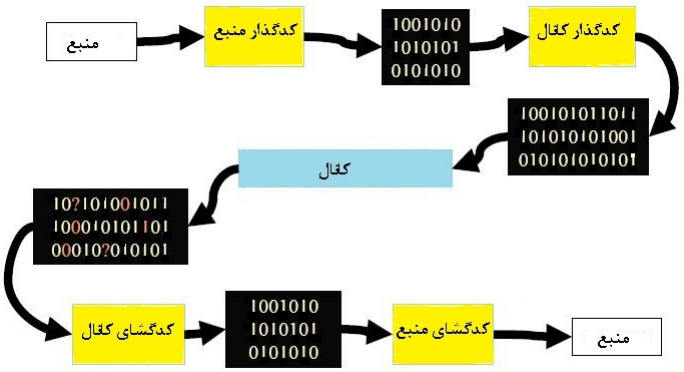
[۱] Claude Shannon
[۲] Information theory
[۳] R.W. Hamming
[۴] Coding theory
[۵] Theory of Error-Correcting Codes
[۶] Source coding theory
[۷] Channel coding theory



شکل ۱.۱: برخی از رویدادهای مهم در کدگذاری

نظریه کدگذاری شانون ادعا و به صورت نظری اثبات می‌کند که برای هر کانال، ماکزیمم نرخی وجود دارد که در آن نرخ می‌توان داده‌ها را به گونه‌ای که احتمال خطا صفر شود، مخابره کرد. این ماکزیمم نرخ به **ظرفیت کانال** [۸] مشهور شده است. علاوه براین شانون اثبات می‌کند که تقریبا هر کد بسیار بزرگ، می‌تواند به این ظرفیت برسد. البته این اثبات، چگونگی ساخت این کدها و نحوه **کدگذاری** [۹] و **کدگشایی** [۱۰] آنها را بیان نمی‌کند. در حقیقت یک کد تصادفی به اندازه دلخواه بزرگ ممکن است با استفاده از اصول فنی به خوبی اجرا شود ولی زمان‌های (پیچیدگی زمانی) کدگذاری و کدگشایی آن ممکن است بسیار بزرگ باشند. به این ترتیب (پس از کارهای شانون) یکی از اهداف اصلی نظریه کدگذاری، ساخت کدهایی شد که با پیچیدگی کدگذاری و کدگشایی قابل کنترل به ظرفیت کانال می‌رسند. از جمله موفقیت‌هایی که در نتیجه این تلاش‌ها حاصل شد، ساخت کدهای **توربو** [۱۱] در سال ۱۹۹۳ [۷] بود با ساخت این کدها، **کدگشایی تکراری** [۱۲] (که باعث اجرای عالی و پیچیدگی پایین گردید) مطرح شد. پس از آن **کدهای LDPC** [۱۳] دوباره مطرح شدند (قبل از آن توسط گالاگر در سال ۱۹۶۲ کشف

[۸] Capacity of channel
[۹] Encoding
[۱۰] Decoding
[۱۱] Turbo code
[۱۲] Iteration decoding
[۱۳] Low-density parity-check codes



شکل ۲.۱: سیستم ارتباطی

شده بود) .

آنچه با کار شانون از سال ۱۹۴۸ آغاز شد را به طور خلاصه می‌توان در شکل ۱.۱ دید. در فاصله زمانی ۱۹۴۸ تا ۱۹۹۳ (قبل از کدهای توربو) کدهایی با ساختار جبری از جمله کدهای خطی (که توسط الیاس [۱۴] کشف شد) مطرح شدند. پس از آن کدهای خوبی مانند **ریدمولر**[۱۵] و **کدهای پیچشی**[۱۶] ارائه شدند.

آنچه در این فصل ارئه می‌شود عبارت است از: در بخش ۲.۱ سیستم ارتباطی شرح داده می‌شود. در بخش ۳.۱ کانال‌های ارتباطی مورد نیاز تعریف می‌شوند. در بخش ۴.۱ فرضیاتی که در این پایان‌نامه مورد استفاده قرار می‌گیرند بیان می‌شوند. در بخش ۵.۱ مقیاس گذاری LLR برای کانال‌های مورد نظر بیان می‌گردد.

۲.۱ سیستم ارتباطی

همانطور که در شکل ۲.۱ می‌بینید ، در یک سیستم ارتباطی یک پیام (از منبع) ابتدا توسط کدگذار منبع، کدگذاری (رمزگذاری) می‌گردد (در شکل ۲.۱ الفبای کدگذاری میدان دودویی در نظر گرفته شده است ولی می‌تواند تغییر کند) . حاصل این عمل، برداری به طول k است. سپس کدگذار کانال به این بردار با توجه به مدل کدگذاری کانال

[۱۴] Elias
[۱۵] Reed-Muller
[۱۶] Convolutional codes

مورد نظر **افزونگی**[۱۷] اضافه می‌کند. که این افزونگی موجب می‌شود که کدگشای کانال بتواند خطای حاصل از پارازیت کانال را در صورت امکان کشف و تصحیح کند. بردار جدید حاصل از مرحله کدگذاری کانال را **کدواژه**[۱۸] می‌نامند که عنصری متعلق به $F_۲^n$ (با فرض الفبای دودویی $GF(۲)$ یا $F_۲$) است. به این ترتیب k را **بعد** (اندازه) کد و n را **طول کد** (طول کدواژه) می‌نامند. کدواژه از طریق کانال ارسال می‌گردد. کانال معمولا خواصی دارد که (این خواص) موجب تغییر سیگنال‌هایی که از کانال عبور می‌کنند، می‌گردند و آنها را تحریف (خراب) می‌کند. یکی از مواردی که موجب تحریف کدواژه ارسالی می‌گردد وجود پارازیت (نوفه) در کانال است. در انتهای کانال، گیرنده واژه‌ای را از کانال دریافت می‌کند که (با توجه به تغییرات رخ داده در پیام ارسالی در اثر پارازیت) ممکن است کدواژه نباشد. کدگشای کانال، سعی خواهد کرد خطاهای احتمالی واژه دریافتی را در صورت امکان کشف و تصحیح کند و به این ترتیب محتمل‌ترین کدواژه (که به طور محتمل‌تر همان کدواژه ارسالی است) را به کدگشای منبع (رمزگشا) تحویل می‌دهد. کدگشای منبع نیز آن‌را رمزگشایی و پیام اصلی را از آن استخراج می‌کند. به مثال زیر توجه کنید.

مثال ۱.۲.۱. [۲۱] عمل کپی کردن فیلم یا اطلاعات روی DVD را در نظر بگیرید. در این عمل، کامپیوتر به عنوان کدگذار منبع و کدگذار کانال عمل می‌کند. یعنی اطلاعات را به داده‌های دودویی تبدیل می‌کند و با توجه به مدل کدگذاری کانال مورد استفاده افزونگی مورد نیاز را به آن اضافه می‌کند. سپس اطلاعات را روی DVD کپی می‌کند. در اینجا DVD، کانال است. DVDممکن است خراشیده یا کثیف گردد، به این ترتیب برخی از اطلاعات روی آن خراب خواهند شد. اجراکننده DVD (DVD player) می‌تواند این داده‌ها را تعمیر کند و آنها را بخواند (یعنی به عنوان کدگشای کانال و کدگشای منبع عمل می‌کند).

♢

به این ترتیب می‌توان فرض کرد:

[۱۷] Redundancy
[۱۸] Codeword

- بردار اطلاعات: $u = \left[\begin{array}{ccc} u_۱ & \dots & u_k \end{array} \right]^T \in F_۲^k$
- کدواژه: $x = \left[\begin{array}{ccc} x_۱ & \dots & x_n \end{array} \right]^T \in \mathcal{C}$ ، که $x \in F_۲^n$ و $\mathcal{C}$ مجموعه همه کدواژه‌های (مجاز) است، به طوری که $|\mathcal{C}| = ۲^k$ (برای کدهای خطی که در فصل بعد بیان خواهد شد) یعنی:

$$\mathcal{C} = \{x : \ \ x = enc(u) \ , \ u \in F_۲^k\}$$

(منظور از $enc(u)$ کدگذاری u است).

- واژه دریافتی $y = \left[\begin{array}{ccc} y_۱ & \dots & y_n \end{array} \right]^T$ ، مجموعه الفبای y به کانال مورد استفاده وابسته است.
- کدواژه برآورد شده $\hat{x} = \left[\begin{array}{ccc} \hat{x}_۱ & \dots & \hat{x}_n \end{array} \right]^T \in F_۲^n$
- بردار اطلاعات برآورد شده $\hat{u} = \left[\begin{array}{ccc} \hat{u}_۱ & \dots & \hat{u}_k \end{array} \right]^T \in F_۲^k$
- نرخ کد: $R = k/n$ (برای کدهای خطی که در فصل بعد بیان خواهد شد).

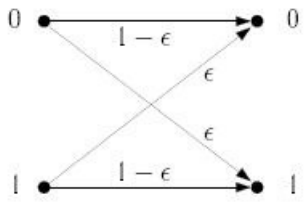
۳.۱ مدل‌های کانال مورد استفاده در این پایان‌نامه

تعریف ۱.۳.۱. یک کانال را **بی‌حافظه**[۱۹] گویند اگر خروجی کانال در هر لحظه فقط به ورودی کانال در همان لحظه وابسته باشد. به عبارت دیگر اگر $y = y_۱, \dots, y_n$ خروجی و $x = x_۱, \dots, x_n$ ورودی باشد آنگاه:

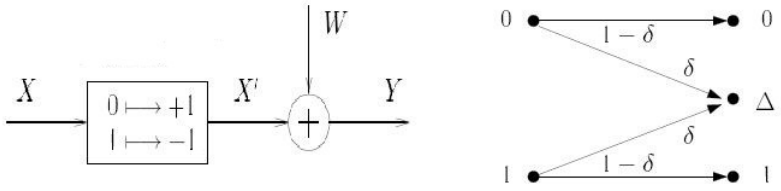
$$p(y|x) = \prod_{i=۱}^{n} p(y_i|x_i) \qquad (۱.۱)$$

در این حالت کانال به طور کامل توسط الفبای ورودی و خروجی شرح داده می‌شود.

[۱۹] Memoryless



شکل ۱.۳: BSC با احتمال همگذری ϵ



شکل ۱.۴: نمودار سمت راست BECبا احتمال پاکشدگی کانال δ و نمودار سمت چپ کانال (BI-AWGNC) نرمال شده است.

تعریف ۱.۳.۲. کانال متقارن دودویی (BSC)[۲۰] ، کانالی ورودی دودویی، خروجی دودویی با پارامتر ϵ است که در آن $p(۰|۱) = p(۱|۰) = \epsilon$ و $p(۱|۱) = p(۰|۰) = ۱ - \epsilon$ است و به ϵ **احتمال همگذری**[۲۱] می گویند.

به نمودار (۳.۱) توجه کنید.

تعریف ۱.۳.۳. کانال پاک شدگی دودویی BEC[۲۲] کانالی با پارامتر δ است که به آن **احتمال پاک‌شدگی**[۲۳] می گویند و الفبای ورودی آن $\{۰, ۱\}$ و الفبای خروجی آن $\{۰, ۱, ?\}$ است و در آن

$p(۱|۱) = p(۰|۰) = ۱ - \delta$ و $p(?|۱) = p(?|۰) = \delta$ است (منظور از ? بیت پاک‌شده است). به نمودار ۴.۱ توجه کنید.

تعریف ۱.۳.۴. در کانال $(BI\text{-}AWGNC)$ [۲۴] ، ورودی x به $x' \in \{+۱, -۱\}$ نگاشته می‌شود سپس پارازیت سفید نرمال به آن اضافه می‌شود. به این ترتیب خروجی $y = x' + w$ است که $w \sim \mathcal{N}(۰, N_۰/۲E_s)$. الفبای

[۲۰] Binary Symmetric Channel
[۲۱] Cross over probability
[۲۲] Binary Erasure Channel
[۲۳] erasure probability
[۲۴] Binary Input Additive White Gaussian Noise Channel

خروجی این کانال $y \in \mathbb{R}$ است. به نمودار ۴.۱ توجه کنید) $N_0/2E_s$ نسبت سیگنال به پارازیت هر نماد کد (SNR) است).

۱.۳.۱ نسبت‌های درستنمایی

یکی از مفاهیمی که در این پایان‌نامه به دفعات مورد استفاده قرار می‌گیرد، **لگاریتم نسبت درستنمایی (LLR)**[۲۵] است که به صورت زیر تعریف می‌شود:

$$l = \lambda_i = L(y_i|x_i) = \ln\left(\frac{p(y_i|x_i = 0)}{p(y_i|x_i = 1)}\right) \qquad (۲.۱)$$

مقدار l ، میزان قطعی بودن اینکه x ، ۰ یا ۱ است را شرح می‌دهد. اگر l مثبت باشد آنگاه

$$p(y_i|x_i = 0) > p(y_i|x_i = 1)$$

و باید $\hat{x} = 0$ باشد. به همین ترتیب اگر l منفی باشد آنگاه

$$p(y_i|x_i = 0) < p(y_i|x_i = 1)$$

و $\hat{x} = 1$. هرچه مقدار $|l|$ بزرگتر باشد آنگاه قابلیت اطمینان نماد، بیشتر خواهد بود.

قانون تصمیم سخت l عبارت است از:

$$\hat{x} = \begin{cases} 0 & l \geq 0 \\ 1 & l < 0 \end{cases}$$

به این ترتیب مقدار l برای کانالهای تعریف شده در این فصل به صورت زیر است:

- BSC :

$$L_{BSC}(y_i|x_i) = \begin{cases} \ln\left(\frac{1-\epsilon}{\epsilon}\right) & y_i = 0 \\ \ln\left(\frac{\epsilon}{1-\epsilon}\right) & y_i = 1 \end{cases}$$

[۲۵] Log likelihood ratio