دانشکده مهندسی

گروه برق

پایان‌نامه کارشناسی

گرایش: مخابرات

عنوان :

بررسی کدهای ال دی پی سی و کاربردهای آن

استاد راهنما: آقای دکتر محمد مصطفوی

نگارش: اردشیر علیمحمدی

شهریور92

چکیده

امروزه رمزهای ال دی پی سی[1] یکی از موضوعات جنجال برانگیز در نظریه رمزنگاری هستند. آنها در اوایل دهه 1960 پایه ریزی شدند ولی بازگشتی شگفت انگیز در چند سال گذشته را تجربه کرده اند. برخلاف بسیاری از طبقات دیگر از رمزها، رمزهای ال دی پی سی در حال حاضر با روندی بسیار سریع (به صورت احتمالی) مجهز به الگوریتم های رمزنگاری و رمزگشایی شده اند. سوال این است که با طراحی این رمزها با این الگوریتم آیا می توان در صورت همراه شدن اغتشاشات به رمز اصلی دست پیدا کرد؟ روش های تحلیلی جدید و ابزار هایی ترکیبی این مشکل را قادر است برطرف سازند. این باعث می شود رمزهای ال دی پی سی نه تنها از نقطه نظر تئوری جذاب باشند، بلکه برای کاربردهای عملی نیز مناسب باشند. الگوریتم های استفاده شده برای دیکدینگ کدهای ال دی پی سی به صورت مستقلانه در زمان های مختلف کشف شده اند(به دست آمده اند).و حقیقت امر این است که به اسم های گوناگون گرد آمده اند.عمونی ترین آنها(مشترک ترین) "الگوریتم انتشار بیلیف " و "الگوریتم پیام گذرنده " و "الگوریتم سام-پروداکت[2] " میباشند.

کدهای ال دی پی سی در سالهای گذشته مورد مطالعه قرار گرفته و پیشرفتهای عظیم و چشم گیری در فهم و توانایی این کدها در جهت طراحی سیستم های کدینگ تکرارشونده به دست آمده است.روشهای کدینگ های تکرارشونده در گذشته برای کدهای توربو استفاده میشد اما ساختار کدهای ال دی پی سی نتایج بهتری را ارائه میدهند.علاوه بر این موضوع این کدها ساختن دیکدرهای موازی را ممکن کردند.مهم ترین اشکال این کدها به نوعی پچیده بودن کدینگ آنها و همچنین بیش از حد طولانی بودن طول کدها در مقابل بازده خوب آنهاست.

در این قسمت به مروری کوتاه به ریشه رمزهای ال دی پی سی می پردازیم و روش هایی که برای تجزیه و تحلیل و طراحی آنها استفاده می شود را بیان می نماییم.

---

[1] LDPC
[2] sum-product algorithm

فهرست

عنوان **صفحه**

مقدمه ای از کدینگ و دیکدینگ

1.1نظریه شانون

سال 1948 آغاز تولد تئوری اطلاعات است. در آن سال، کلود شانون[3] مقاله سازنده عصر خود را منتشر ساخت که در آن از محدودیت های انتقال قابل اعتماد داده ها بر روی کانال های غیر قابل اعتماد و شیوه های مواجهه با این محدودیت ها سخن به میان آورد. در میان مقالات دیگر، این مقاله به طور رسمی منجر به درک مفهوم اطلاعات و مرزهایی را برای حداکثر اطلاعاتی که قادر است بین کانال های غیرقابل اعتماد انتقال یابد تاسیس کرد.

یک کانال ارتباطی معمولا به عنوان یک عنصر سه گانه که متشکل از الفبای ورودی، الفبای خروجی، و برای هر جفت (i,o) از عناصر ورودی و خروجی شامل یک انتقال احتمالی$p(i,o)$ است، تشکیل می شود. به صورت معنایی، انتقال احتمالی ، احتمالی است که نماد o دریافت می شود زمانی که i در سمت دیگر کانال ارسال شده باشد.

با توجه به یک کانال ارتباطی، شانون نشان داد که یک عدد به نام ظرفیت کانال وجود دارد، به طوری که انتقال قابل اعتماد اطلاعات برای نرخهای اختیاری نزدیک به ظرفیت ممکن است و انتقال قابل اعتماد اطلاعات برای نرخهای بیشتر از ظرفیت امکان پذیر نیست.

مفهوم ظرفیت صرفا در چارچوب تئوری اطلاعات بیان می گردد. البته آن دستیابی به طرح های انتقالی که منجر به پر شدن ظرفیت شود را تضمین نمی کند. در همان مقاله شانون به معرفی مفهوم رمزهایی که به عنوان گروه بردار باید انتقال یابند پرداخت. در ذیل من برای ایجاد انگیزه به مقوله مفهوم خواهم پرداخت. روشن است که اگر در کانال حتی اگر یک عنصر ورودی را بتوان در حداقل دو راه ممکن

[3] Claude E. Shannon

دریافت کرد (البته با احتمالات متفاوت) ، باید فقط عناصر مجردی بر روی کانال فرستاده شود تا ارتباط قابل اعتماد در آن کانال امکان پذیر شود. این امر حتی برای حالتی صادق است که عناصر مختلفی فرستاده شوند ولی امکان ارتباط معناداری در آنها مشاهده نشود (به شیوه دقیق ساخته شده باشد). برای دستیابی به ارتباطات قابل اعتماد، ضروری است که عناصر ورودی باید با یرمزیگر ارتباط داشته باشند. این منجر به مفهوم یک رمز خواهد شد، که به عنوان (متناهی) مجموعه ای از بردارها بیش از الفبای ورودی تعریف می گردد. ما فرض می کنیم که تمام بردارها طول یکسانی دارند، و این طول را *طول بلوک* رمز نامگذاری می کنیم. اگر تعداد بردارها $K = 2^K$ باشد، پس از آن هر بردار را می توان با k بیت نمایش داده شود. اگر طول بردار n باشد، در n دفعه استفاده از کانال k بیت منتقل شده است.

سپس می توانیم بگوییم رمز دارای نرخ k/n بیت در استفاده از کانال، یا k/n bpc[4] می باشد.

فرض کنید که ما یک رمز واژه[5] ارسال کنیم و یک بردار بیش از الفبای خروجی دریافت کنیم. چگونه می توانیم از بردار به چیزی که در ابتدا فرستادیم دست یابیم؟ اگر کانال به خطا ها اجازه عبور دهد، بنابراین هیچ راه کلی برای استنباط از رمز واژه به طور قطع یقین وجود ندارد. اگرچه ، ما می توانیم رمز واژه احتمالی را که فرستاده شده است با شرطی که احتمال ارسال این رمز واژه به بردار مشاهده به صورت ماکزیمم باشد، حدس بزنیم. برای اینکه بتوانیم چنین رمزواژه را پیدا کنیم، به سادگی می توان با تهیه لیستی از تمام K رمزواژه، و محاسبه احتمال شرطی برای هر یک از رمزواژه ها آن ها را پیدا کنیم. سپس با یافتن بردار و یا بردارهایی که منجر به حداکثر احتمال می شود، یکی از آنها را ارجاع دهیم. این شیوه رمزگشایی محتمل ترین شیوه رمزگشایی می باشد. البته این کامل نیست: مدت زمان زیادی طول می کشد (به ویژه هنگامی که رمز طولانی است) و ممکن است همراه با خطا باشد، اما این بهترین کاری است که می توانیم انجام دهیم.

---

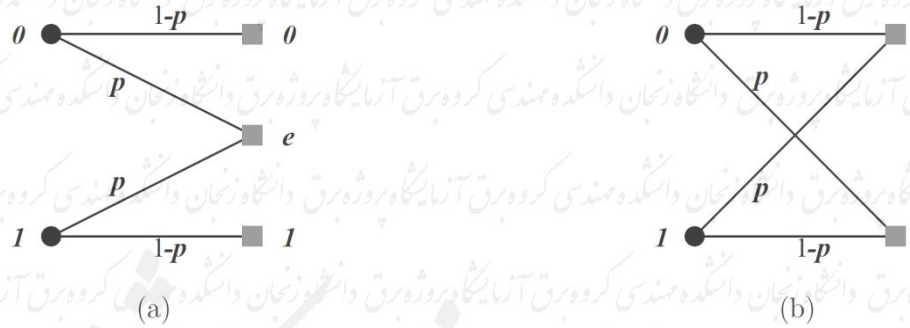
[4] Bit Per Channel
[5] codeword

شانون وجود رمزهایی با نرخ اختیاری نزدیک به ظرفیت را که احتمال وجود خطا در آنها به صورت ماکزیمم است که احتمال رمزگشایی در آنها به صفر و در طول، این بلوک ها به بینهایت می رود را اثبات نمود.(در واقع، شانون ثابت کرد که خطای رمزگشایی از حداکثر احتمال رمزگشایی، به صورت نمایی و سریع با طول بلوک به صفر می رود، اما این قضیه در اینجا مورد بحث نیست.)

رمزهایی که به سطح ظرفیت می رسند از رویکرد ارتباطی بسیار خوبی برخوردار می باشند ، اما نظریه شانون غیر سازنده است و راه حلی برای دستیابی به این رمز ها ارائه نمی دهد. مهمتر از آن، حتی اگر به صورت پیشگویی شده توالی رمزهایی را که در یک نرخ خاص به ظرفیت نزدیک می شوند را داشته باشیم، روشن نیست که چگونه باید برای رمزنگاری و رمزگشایی آنها اقدام کنیم؟ طراحی رمزها با الگوریتم های موثر رمزنگاری و رمزگشایی که از تمام ظرفیت کانال استفاده کند موضوع اصلی این نوشتار می باشد.

قبل از اینکه من این بخش را پایان دهم، اجازه دهید من یک مثال از دو کانال ارتباطی بیان کنم: کانال λ دودویی[6] ، و کانال دودویی متقارن[7]. این کانال ها در شکل 1 توضیح داده شده اند. در هر دو مورد الفبای ورودی دودویی است، و عناصر الفبای ورودی بیت نامیده می شوند. در کانال حک دودویی الفبای خروجی شامل 0، 1 و یک عنصر اضافی که با e نشان داده می شود و بنام حک نام گذاری شده است. هر بیت یا به درستی منتقل می شود (با احتمال $p-1$)، و یا پاک می شود (با احتمال p). ظرفیت این کانال $p-1$ می باشد.

[6] Binary Eآر ایsure Channel
[7] Binary Symmetric Channel



شکل 1: دو نمونه از کانال: (الف) کانال حک دودویی با احتمال p حک، و (ب) کانال دودویی متقارن با احتمال خطای p.

در کانال دودویی متقارن هر دو ورودی و خروجی الفبای F2 هستند .هر بیت یا به درستی با احتمال $1-p$ منتقل می شود یا با احتمال p معکوس می شود.این کانال ممکن است در وهله اول ممکن است ساده تر از کانال حک دودویی به نظر برسد، اما در واقع بسیار پیچیده تر از آن است. مشکلات از آنجا ناشی می شود که مشخص نیست رمزام بیت ها معکوس شده است. (در مورد کانال دودویی متقارن روشن است که رمزام بیت پاک شده است.)

ظرفیت این کانال $1 + p\log_2(p) + (1-p)\log_2(1-p)$ است. حداکثر احتمال رمزگشایی برای این کانال معادل با یافتن طول بردار n خارج از F2 است، یا رمز واژه ای است که از کلمه دریافتی کوچکترین فاصله همینگ[8] را داشته باشد. می توان نشان داد که حداکثر احتمال رمزگشایی برای کانال دودویی متقارن به صورت NP کامل می باشد. برخلاف آن برای رمز های خطی حداکثر احتمال رمزگشایی در کانال حک دودویی به صورت سری های زمانی چند جمله ای می باشد که این امر باعث کاهش دادن زمان در سیستم های معادلات این کانال ها می شود.

2.1مسائل الگوریتمی

[8] Hamming

بلافاصله پس از اکتشافات شانون محققان نشان دادند که رمزهای تصادفی می توانند به ظرفیت برسند. در واقع، این موضوع به صورت ضمنی در رساله شانون بیان شده بود.

اما دستیابی به ظرفیت تنها بخشی از داستان است. اگر این رمز ها برای برقراری ارتباط مورد استفاده قرار گیرد، نیاز به الگوریتم های سریع برای رمزنگاری و رمزگشایی است. توجه داشته باشید که رمزهای تصادفی از نرخ R بیت بر کانال بردارهای تصادفی به تعداد 2^{Rn} و به طول n بیش از الفبای ورودی را تشکیل می دهند. ما نیاز به برخی جزئیات از بردارها داریم تا قادر به جاسازی اطلاعات در داخل آنها شویم، و یا نیاز داریم همه آنها را برای تشکیل کتاب رمزینه بنویسیم. این کتاب حاوی فهرست هایی از بیت های Rn می باشد که به هر رمز واژه مرتبط شده است. این کتاب رمز نیازمند گنجایش 2^{Rn} است که به طور معقول بسیار بزرگ به نظر می رسد (با طول 1000 و نرخ 0.5 که 2^{500} بردار را تولید می کند – برای پردازش بسیار بزرگ است).

اگر الفبای ورودی دارای ساختار میدانی باشد (برای مثال الفبای دودویی که حاصل آن میدان F2 است)، می توان بهترین کار را انجام داد یا حداقل تا جایی که رمزنگاری پیش رود. الیاس و گولای[9] به طور مستقل مفهوم رمزهای خطی بلوک با طول n و بعد k را به عنوان زیر فضاهای فضای برداری F_2^n، معرفی کردند. بعضی از رمز ها با نرخ k/n (ما واحد bpc برای رمزهای دودویی از حالا به بعد حذف می کنیم)، و از آنجایی که آنها خطی هستند، آنها را می توان به صورت پایه با k بردار با طول n شرح داد. یک کتاب رمزینه را می توان به صورت ضمنی و به شیوه طبیعی توسط نگاشت یک بیت بردار $(x_1, \dots, x_k)$ به بردار دیگر ، با کمک ترکیب خطی بردار پایه داده شده بوسیله ضرایب $(x_1, \dots, x_k)$ تشریح کرد.

طبقه رمز های خطی بسیار غنی است. استدلال شانون می تواند مورد استفاده قرار گیرد (تقریبا کلمه به کلمه) تا نشان دهد که توالی رمزهایی با نرخ اختیاری نزدیک به ظرفیت با وجود احتمال خطای

[9] Elias and Golay

ماکزیمم، که احتمال رمزگشایی در آنها به صفر و طول، این بلوک ها به بینهایت می رود؛ موجود است. علاوه بر این، همچنین می تواند نشان داد که رمزهای خطی تصادفی توانایی رسیدن به ظرفیت را دارد. بر خلاف رمز های غیر خطی مرتبط، رمز های خطی را می توان در زمان چند جمله ای به نسبت زمان های نمایی رمز نگاری کرد، که این خبر خوبی است.

د رمزگشایی چگونه است؟ رمز گشایی به نظر بسیار سخت تر می رسد. همانطور که در بالا ذکر شد، مشکل احتمال حداکثر در کانال دودویی متقارن برای کلاس های بسیاری از رمز های خطی به صورت NP-سخت نشان داده شده است (به عنوان مثال، رمز های عمومی خطی بیش از F_q برای هر q تولید می شوند). بنابراین بعید به نظر می رسد که بتوانیم الگوریتم های زمانی چند جمله ای را برای حداکثر احتمال رمزگشایی رمزهای عمومی خطی پیدا کنیم. یکی از راههای غلبه به این نتیجه منطقی تلاش در تکرار آزمون های موفق برای مشکل رمزنگاری است و بویژه در زیرمجموعه رمز های عمومی خطی. با این حال، ما قادر نشده ایم تا زیر مجموعه رمز های خطی را برای احتمال رمزگشایی حداکثری که زمان چند جمله ای دارند و به ظرفیت می رسند پیدا کنیم.

احتمال دیگر این است که از الگوریتم های بهینه فرعی که دارای زمان چند جمله ای بوسیله ساختار خود می باشند را در نظر بگیریم.

3.1تحلیل طول-محدود[10]

یک گراف دو قسمتی داده شده که مربوط به رمز است، و مجموعه ای از حک شونده ها در میان گره های چک را فرض کنید، این گراف را القا شده از گره های پیام های پاک شده در نظر بگیرید. یک مجموعه *متوفق کننده* در این گراف، مجموعه ای از گره های پیامی می باشد که توسط گره های پیام به گراف القا شده است، در این گره ها ، هیچ گره چکی از درجه یک نیست.

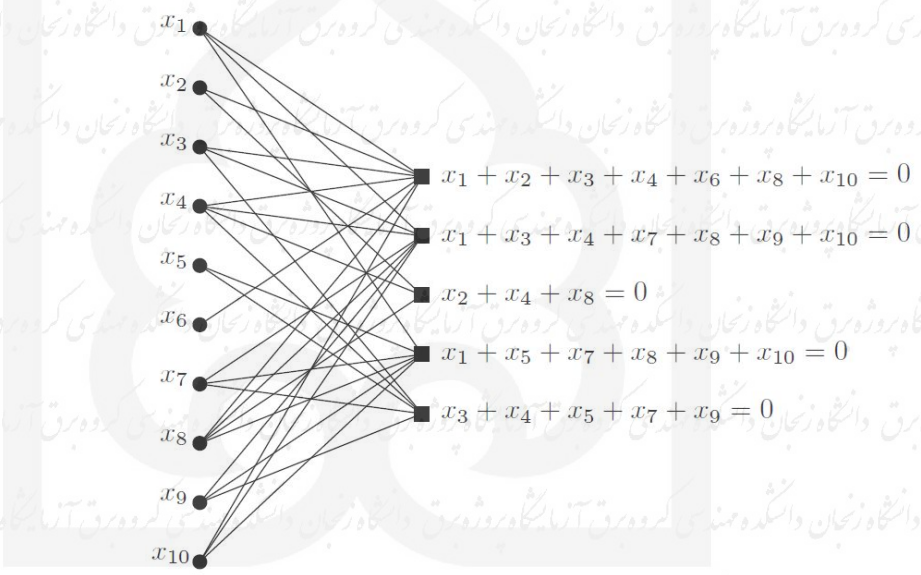
[10] Finite-Length Analysis

تعداد گره های پیام در مجموعه متوقف کننده ، اندازهٔ آن نامیده می شود. انتشار باور در کانال حک دودویی ، اگر و فقط اگر این زیرگراف دارای مجموعه متوقف کننده باشد ، به طور دائمی متوقف خواهد شد. شکل 5 نمونه ای از گراف هایی است که خودشان دارای مجموعه متوقف کننده می باشند. چون اجتماع مجموعه های متوقف کننده ، مجموعه های متوقف کننده می باشد ، هر گراف محدود که شامل یک مجموعه متوقف کننده ماکزیمم است. (که ممکن است مجموعه تهی باشد). برای گراف های دو قسمتی احتمال آنکه انتشار باور بر روی کانال حک دودویی گره های پیام l را در نقطه عیب، بازیابی نکند، با احتمال آنکه گرافی که از گره های پیام حذف شده در مجموعه متوقف کننده ماکزیمم با اندازه l تولید شده باشد، برابر است.

ال دی پی سی چیست؟

1.2رمز های ال دی پی سی

رمزهای ال دی پی سی توسط رابرت گالاگر[11] و در پایان نامه دکترای او ابداع شد. بلافاصله پس از ابداع او، آنها به طور گسترده ای به دست فراموشی سپرده شدند و چندین بار دیگر تا 30 سال بعد دوباره ابداع گردیدند. باز گشت آنها، یکی از جذاب ترین جنبه های تاریخ خود می باشد زیرا دو انجمن متفاوت، به دلایل متفاوت در زمان های یکسان دست به ابداع رمزهایی شبیه به رمزهای ال دی پی سی گالاگر زدند.



شکل 2 : یک رمز ال دی پی سی

رمزهای ال دی پی سی رمز های خطی هستند که از گراف های دو قسمتی پراکنده به دست آمده اند. فرض کنید که یک گراف با n گره چپ (به نام گره های پیام) و r گره راست (به نام گره چک) باشد. حاصل این گراف یک رمز خطی با طول بلوک n و ابعاد حداقل $n - r$ به صورت زیر می باشد:

[11] Robert Gallager

nمختصات رمزواژه ها با گره های پیام مرتبط می باشند. رمزواژه های آن بردارها $(c_1, \dots, c_n)$ مثلا برای تمام گره های چک، با مجموع برخی از گره های همسایه یا گره های پیام باید برابر با صفر باشد. شکل 2 مثالی در این زمینه بیان می دارد.

گراف بیانگر ماتریس مجاوری می باشد که می توان با مشاهده در گراف آنرا بدست آورد: فرض کنیم H ماتریسی دودویی با فضای r x n باشد. درایه (i,j) یک می باشد اگر و فقط اگر i امین گره چک در گراف به j امین گره پیام متصل می شود. سپس می توان رمز ال دی پی سی را طوری توسط گراف تعریف کرد که مجموعه ای از بردارها به صورت $c = (c_1, \dots, c_n)$ باشد که رابطهٔ $H.c^T = 0$ برقرار باشد. ماتریس H یک ماتریس چک زوجیت برای رمز نام گذاری می شود. به صورت عکس هر دودویی در ماتریس r x n نشان دهنده یک گراف دو قسمتی بین n پیام و r گره چک می باشد، و رمز به عنوان فضای تهی از H که دقیقا به این گراف مرتبط است تعریف می گردد. بنابراین، هر گونه رمز خطی نماینده رمزی مرتبط شده بین گراف های دو قسمتی گراف می باشد. (توجه داشته باشید که این گراف توسط این رمز منحصر به فرد تعریف نمی شود). با این حال، نمی توان گفت هر رمز خطی دودویی نماینده یک گراف دو قسمتی پراکنده می باشد[12]. اگر این چنین باشد، این رمز یک رمز آزمون جفت متعادل با تراکم کم یا ال دی پی سی نامیده می شود. پراکندگی ساختار گراف یک خاصیت کلیدی می باشد که به بازده الگوریتم رمز های ال دی پی سی کمک می کند.

کدهای ال دی پی سی از دسته کدهای خطی میباشند.این نامگذاری از مشخصه های بررسی توازن ماتریسهایی که شامل تنها مقدار کمی 1 در مقایسه با تعداد 0 های آنهاست آمده است.مزیت اصلی این نوع کدها در دسترسی قرار دادن یک کارآیی مهم که همان کم کردن حجم بسیاری از کانالها و الگوریتم های پیچیده و مختلط متغییرهای خطی وابسته به زمان برای دیکدینگ می باشد.اما بسبب خطا کردن در پروسه تلاش برای تکمیل کردن کدینگ و دیکدینگ برای بسیاری از کدها و همچنین

[12] به عبارت دقیق تر، پراکندگی تنها به سلسله ای از ماتریس ها اعمال می شود. دنباله ای از ماتریس های $n \times m$ مجموعه پراکنده c نامیده می شوند اگر حاصلضرب mn به سمت بی نهایت رود و تعداد عناصر غیر صفر در این ماتریس همیشه کمتر از c ماکزیمم در درایه های (m,n) باشد.

تلاش بر روی مقدمه ای از کدهای "رید-سالمون" این کدها تا 10 سال گذسته کاملا فراموش شده بودند.

این دسته از کدها 2 امکان مختلف جهت نمایش دادن کدهای ال دی پی سی دارند.مانند تمام کدهای بلوکی خطی آنها هم می توانند توسط ماتریسها توصیف شوند.امکان دیگر نمایش گرافی آنها می باشد.

2.2نمایش ماتریسی

ماتریس تعریف شده در شکل 3 یک ماتریس بررسی توازن با ابعاد $n \times m$ برای یک کد 4×8 می باشد.الان ما می توانیم 2 نوع شرح دادن را برای این ماتریس تعریف کنیم:wt برای 1 ها در هر سطر و wc برای ستونها.برای اینکه یک ماترس "چکاتی پایین" نامیده شود باید دو شرط زیر برقرار باشد.

در شکل 1.3 گراف "تنز" با ماتریس توازن مطابق است.مسیر علامتگذاری شده $c2 \rightarrow f1 \rightarrow c0 \rightarrow f2 \rightarrow c2$ نمونه ای از چرخه کوتاه میباشد.

شکل 3 $H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

4.مراجع [28] و مواخذ

[1] C. E. Shannon, “A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379-423, 1948.

[2] E. Berlekamp, R. McEliece, and H. van Tilborg, “On the inherent intractability of certain coding problems," *IEEE Trans. Inform. Theory*, vol. 24, pp. 384-386, 1978.

[3] P. Elias, “Coding for two noisy channels," in *Information Theory*, Third London Symposium, pp. 61-76, 1955.

[4] R. G. Gallager, *Low Density Parity-Check Codes*. MIT Press, Cambridge, MA, 1963.

[5] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers, Inc., 1988.

[6] M. Luby, M. Mitzenmacher, and A. Shokrollahi, “Analysis of random processes via and-or tree evaluation," *in Proceedings of the 9th Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 364-373, 1998.

[7] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, “Analysis of low density codes and improved designs using irregular graphs," *IEEE Trans. Inform*. Theory, vol. 47, pp. 585-598, 2001.

[28] References

[8] T. Richardson and R. Urbanke, “The capacity of low-density parity check codes under message- passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599-618, 2001.

[9] T. Richardson, A. Shokrollahi, and R. Urbanke, “Design of capacity-approaching irregular low- density parity-check codes," *IEEE Trans. Inform*. Theory, vol. 47, pp. 619-637, 2001.

[10] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, “Efficient erasure correcting codes," *IEEE Trans. Inform. Theory,* vol. 47, pp. 569-584, 2001.

[11] M. Luby, M. Mitzenmacher, A. Shokrollahi, D. Spielman, and V. Stemann, “Practical loss- resilient codes," *in Proceedings of the 29th annual ACM Symposium on Theory of Computing*, pp. 150-159, 1997.

[12] L. Bazzi, T. Richardson, and R. Urbanke, “Exact thresholds and optimal codes for the binary symmetric channel and Gallager's decoding algorithm A," *IEEE Trans. Inform. Theory,* vol. 47, 2001.

[13] A. Shokrollahi, “New sequences of linear time erasure codes approaching the channel capacity," *in Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes* (M. Fossorier, H. Imai, S. Lin, and A. Poli, eds.), no. 1719 in Lecture Notes in Computer Science, pp. 65-76, 1999.

[14] V. V. Zyablov and M. S. Pinsker, “Estimation of error-correction complexity of Gallager low- density codes," *Probl. Inform. Transm.*, vol. 11, pp. 18-28, 1976.

[15] M. R. Tanner, “A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, pp. 533-547, 1981.

[16] M. Sipser and D. Spielman, “Expander codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1710- 1722, 1996.

[17] D. Spielman, “Linear-time encodable and decodable error-correcting codes," *IEEE Trans. In- form. Theory*, vol. 42, pp. 1723-1731, 1996.

[18] D. Burshtein and G. Miller, “Expander graph arguments for message-passing algorithms," *IEEE Trans. Inform. Theory*, vol. 47, 2001.

[19] S.-Y. Chung, D. Forney, T. Richardson, and R. Urbanke, “On the design of low-density parity- check codes within 0.0045 dB of the Shannon limit," *IEEE Communication Letters*, vol. 5,pp. 58-60, 2001.

[20] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege, “A digital fountain approach to reliable distribution of bulk data," in *proceedings of ACM SIGCOMM '98*, 1998.

[21] P. Oswald and A. Shokrollahi, “Capacity-achieving sequences for the erasure channel," *IEEE*

Trans. Inform. Theory, vol. 48, pp. 3017-3028, 2002.

[22] N. Alon, S. Hoory, and N. Linial, “The Moore bound for irregular graphs." To appear, 2002.

[23] B. Bollobas, *Extremal Graph Theory*. Academic Press, 1978.

[24] G. A. Margulis, “Explicit group-theoretic constructions of combinatorial schemes and their ap- plications in the construction of expanders and concentrators," *Problems of Information Trans- mission*, vol. 24, no. 1, pp. 39-46, 1988.

[25] A. Lubotzky, R. Phillips, and P. Sarnak, “Ramanujan graphs," Combinatorica, vol. 8, no. 3, pp. 261-277, 1988.

[26] J. Rosenthal and P. Vontobel, “Construction of codes using ال دی پی سی Ramanujan graphs and ideas from Margulis," in *Proceedings of the 38th Allerton Conference on Communication, Control, and Computing*, pp. 248{257, 2000.

[27] D. Divsalar, H. Jin, and R. McEliece, “Coding theorems for 'Turbo-like' codes," in *Proceedings of the 1998 Allerton Conference*, pp. 201-210, 1998.

[28] H. Jin, A. Khandekar, and R. McEliece, “Irregular repeat-accumulate codes," in *Proc. 2nd International Symposium on Turbo Codes*, pp. 1-8, 2000.

[29] T. Richardson and R. Urbanke, “E_cient encoding of low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 638-656, 2001.

[30] C. Di, D. Proietti, E. Telatar, T. Richardson, and R. Urbanke, “Finite-length analysis of low- density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48,pp. 1570{1579, 2002.

[31] A. Orlitsky, R. Urbanke, K. Viswanathan, and J. Zhang, “Stopping sets and the girth of tanner graphs," in *Proceedings of the International Symposium on Information Theory*, 2002.

[32] A. Orlitsky and J. Zhang, “Finite-length analysis of ال دی پی سی codes with large left degrees," in *Proceedings of the International Symposium on Information Theory*, 2002.

[33] T. Richardson, A. Shokrollahi, and R. Urbanke, “Finite-length analysis of various low-density parity-check ensembles for the binary erasure channel," in *Proceedings of the International Sym- posium on Information Theory*, 2002.

[34] B. Bollobas, *Random Graphs*. Academic Press, 1985.

[35] M. Molloy and B. Reed, “A critical point for random graphs with a given degree sequence," *Random Structures and Algorithms*, vol. 6, pp. 161-179, 1995. can be downloaded from http://citeseer.nj.nec.com/molloy95critical.html.

[36] M. Molloy and B. Reed, “The size of the giant component of a random graph with a given degree sequence," *Combin. Probab. Comput*., vol. 7, pp. 295-305, 1998. can be downloaded from http://citeseer.nj.nec.com/molloy98size.html.