

## فهرست مطالب

فصل اول: کدبندی برای ذخیره‌سازی و مخابره‌ی امن.....	۱۱
۱-۱ مقدمه.....	۱۳
۲-۱ مفهوم کانال.....	۱۵
۳-۱ اندازه‌گیری اطلاعات و آنتروپی.....	۱۶
۴-۱ ظرفیت کانال.....	۱۷
۱-۴-۱ ظرفیت کانال متقارن باینری و کانال پاک شونددگی.....	۱۸
۲-۴-۱ ظرفیت کانال AWGN.....	۱۸
۵-۱ کدهای بلوکی خطی.....	۱۹
۶-۱ کنترل خطا با استفاده از کدبرداری تصحیح خطا.....	۲۰
۷-۱ کنترل خطا با استفاده از تشخیص خطا و بازارسال اطلاعات.....	۲۰
۸-۱ تمرین‌های فصل اول.....	۲۱
فصل دوم: آشنایی با جبر خطی.....	۲۳
۱-۲ گروه.....	۲۵
۱-۱-۲ تعریف گروه.....	۲۵
۲-۱-۲ تعریف گروه آبلی.....	۲۶
۳-۱-۲ قضایای مربوط به گروه.....	۲۶
۲-۲ زیر گروه.....	۳۰
۱-۲-۲ تعریف زیر گروه.....	۳۰
۲-۲-۲ تعریف همدسته.....	۳۰
۳-۲-۲ قضایای مربوط به همدسته ها.....	۳۱
۳-۲ میدان.....	۳۳
۱-۳-۲ تعریف میدان.....	۳۳
۲-۳-۲ تعریف مرتبه میدان.....	۳۴
۳-۳-۲ قضایای مربوط به میدان.....	۳۴
۴-۲ میدان‌های محدود.....	۳۵
۱-۴-۲ مشخصه میدان محدود.....	۳۶
۲-۴-۲ مرتبه عناصر میدان.....	۳۷
۳-۴-۲ قضایای مربوط به میدان‌های محدود.....	۳۸
۵-۲ چندجمله‌ای‌های باینری.....	۳۹
۱-۵-۲ محاسبات بر روی چند جمله‌ای‌های باینری.....	۴۰
۲-۵-۲ چند جمله‌ای‌های باینری تجزیه ناپذیر و اولیه.....	۴۱
۳-۵-۲ قضایای مربوط به چند جمله ایها.....	۴۳
۶-۲ میدان گالوا $GF(2^m)$ .....	۴۴

۴۸.....	۱-۶-۲ مزدوج عناصر میدان.....
۴۸.....	۲-۶-۲ قضایای مربوط به عناصر میدان $GF(2^m)$ .....
۴۹.....	۷-۲ تجزیه چند جمله‌ای‌های باینری.....
۴۹.....	۱-۷-۲ قضایای مربوط به تجزیه چند جمله‌ای‌ها.....
۵۰.....	۸-۲ چند جمله‌ای‌های حداقلی متناظر با عناصر میدان.....
۵۱.....	۱-۸-۲ تعریف چند جمله‌ای حداقلی.....
۵۱.....	۲-۸-۲ قضایای مربوط به چند جمله‌ای‌های حداقلی.....
۵۴.....	۹-۲ فضای برداری.....
۵۵.....	۱-۹-۲ چند قضیه در مورد فضای برداری.....
۵۶.....	۲-۹-۲ زیرفضای برداری.....
۵۷.....	۳-۹-۲ ترکیب خطی، استقلال خطی و وابستگی خطی.....
۵۸.....	۴-۹-۲ ضرب داخلی در فضای برداری.....
۵۹.....	۵-۹-۲ مجموعه پایه و بعد فضا.....
۵۹.....	۶-۹-۲ زیر فضای دوگان یا پوچ.....
۶۰.....	۷-۹-۲ قضایای مربوط به فضای برداری.....
۶۱.....	۱۰-۲ ماتریس‌های باینری.....
۶۲.....	۱-۱۰-۲ فضای سطری ماتریس.....
۶۴.....	۱۱-۲ تمرین‌های فصل دوم.....

## ۶۷..... فصل سوم: کدهای بلوکی خطی.....

۶۹.....	۱-۳ معرفی کدهای بلوکی خطی.....
۷۰.....	۲-۳ ماتریس مولد و ماتریس آزمون توازن کد خطی.....
۷۵.....	۳-۳ سندروم و آشکارسازی خطا.....
۷۸.....	۴-۳ حداقل فاصله‌ی کد.....
۷۹.....	۱-۴-۳ قضایای مربوط به حداقل فاصله کد.....
۸۱.....	۵-۳ قدرت تشخیص و آشکارسازی خطا در کد بلوکی خطی.....
۸۳.....	۶-۳ محاسبه احتمال خطای آشکارسازی کد با استفاده از توزیع وزنی کد دوگان.....
۸۴.....	۷-۳ قدرت تصحیح خطا در کد بلوکی خطی.....
۸۷.....	۸-۳ آرایه‌ی استاندارد و کدبرداری کد بلوکی خطی.....
۸۹.....	۱-۸-۳ قضایای مربوط به آرایه استاندارد.....
۹۱.....	۲-۸-۳ کدبرداری به کمک آرایه استاندارد.....
۹۳.....	۳-۸-۳ کدبرداری بر اساس سندروم.....
۹۶.....	۹-۳ معرفی چند کد بلوکی خطی ساده.....
۹۶.....	۱-۹-۳ کد آزمون توازن تک بیتی.....
۹۷.....	۲-۹-۳ کد تکرار.....
۹۷.....	۳-۹-۳ کد خود دوگان.....

- ۹۸..... کدهای همینگ ۱۰-۳  
 ۱۰۱..... تمرین‌های فصل سوم ۱۱-۳

### فصل چهارم: کدهای گردش ۱۰۷.....

- ۱۰۹..... ۱-۴ معرفی کدهای گردش  
 ۱۰۹..... ۱-۱-۴ تعریف کدهای گردش  
 ۱۰۹..... ۲-۱-۴ ارتباط جبری بین چندجمله‌ای کد و شیفت گردش آن  
 ۱۱۰..... ۲-۴ قضایای مربوط به ساخت کد گردش  
 ۱۱۲..... ۳-۴ قضایای مربوط به خواص چندجمله‌ای مولد  
 ۱۱۴..... ۴-۴ کد گردش سیستماتیک  
 ۱۱۵..... ۵-۴ ماتریس مولد کد گردش  
 ۱۱۶..... ۶-۴ ماتریس آزمون توازن کد گردش  
 ۱۱۷..... ۷-۴ محاسبه‌ی سندروم و آشکارسازی خطا  
 ۱۱۹..... ۸-۴ کدبرداری کدهای گردش  
 ۱۲۲..... ۹-۴ تحلیل قدرت آشکارسازی کدهای گردش  
 ۱۲۳..... ۱-۹-۴ قضایای مربوط به تحلیل قدرت آشکارسازی کدهای گردش  
 ۱۲۴..... ۱۰-۴ تمرین‌های فصل چهارم

### فصل پنجم: کدهای BCH باینری ۱۲۹.....

- ۱۳۱..... ۱-۵ کدهای اولیه‌ی باینری BCH  
 ۱۳۲..... ۱-۱-۵ درجه چند جمله‌ای مولد و یا تعداد ارقام آزمون توازن  
 ۱۳۶..... ۲-۱-۵ ماتریس آزمون توازن کد BCH  
 ۱۳۸..... ۳-۱-۵ تحلیل قابلیت تصحیح خطای کد BCH اولیه  
 ۱۳۹..... ۲-۵ کدهای BCH باینری غیر اولیه  
 ۱۴۱..... ۳-۵ معرفی کد BCH باینری در حالت کلی  
 ۱۴۱..... ۴-۵ کدگذاری کدهای BCH باینری  
 ۱۴۲..... ۵-۵ کدبرداری کدهای BCH باینری  
 ۱۴۲..... ۱-۵-۵ محاسبه سندروم  
 ۱۴۳..... ۲-۵-۵ تشکیل دستگاه معادلات برای تعیین محل خطا و محاسبه چند جمله‌ای خطا  
 ۱۴۵..... ۶-۵ الگوریتم تکراری برلکمپ برای یافتن چند جمله‌ای خطا  
 ۱۴۸..... ۷-۵ الگوریتم تکراری ساده شده برای یافتن چندجمله‌ای مکان خطای  $\sigma(x)$   
 ۱۵۰..... ۱-۷-۵ یافتن مکان‌های خطا و تصحیح آن  
 ۱۵۱..... ۸-۵ توزیع وزنی و آشکارسازی خطای باینری کدهای BCH  
 ۱۵۵..... ۹-۵ جدول عناصر میدان  $GF(2^6)$   
 ۱۵۷..... ۱۰-۵ تمرین‌های فصل پنجم

## فصل ششم: کدهای Reed-Solomon ..... ۱۶۱

- ۱-۶ مفاهیم پایه در مورد کدهای بلوکی خطی در  $GF(q)$  ..... ۱۶۳
- ۲-۶ کدهای اولیه BCH بر  $GF(q)$  ..... ۱۶۶
- ۳-۶ کدهای Reed-Solomon ..... ۱۶۷
- ۴-۶ کدگذاری کدهای RS ..... ۱۶۸
- ۵-۶ توزیع وزنی کلمات کد RS و تحلیل قابلیت تصحیح خطا ..... ۱۶۸
- ۶-۶ کدبرداری کدهای BCH غیر باینری و RS ..... ۱۷۰
- ۱-۶-۶ الگوریتم کدبرداری برلکمپ ..... ۱۷۰
- ۷-۶ کدبرداری با الگوریتم اقلیدسی ..... ۱۷۶
- ۱-۷-۶ الگوریتم اقلیدسی برای یافتن بزرگترین مقسوم علیه مشترک ..... ۱۷۷
- ۲-۷-۶ حل معادله‌ی کلیدی ..... ۱۷۹
- ۳-۷-۶ خلاصه روش کدبرداری اقلیدسی ..... ۱۸۱
- ۸-۶ کدبرداری در حوزه ی فرکانس ..... ۱۸۲
- ۹-۶ تصحیح خطاها و پاک شدگی‌ها به صورت همزمان ..... ۱۸۹
- ۱۰-۶ تمرین‌های فصل ششم ..... ۱۹۷

## فصل هفتم: کدهای به عنوان کدهای جبری هندسی و کدبرداری لیستی آنها... ۱۹۹

- ۱-۷ تعاریف مورد نیاز ..... ۲۰۲
- ۲-۷ کدهای RS به عنوان کد جبری هندسی ..... ۲۰۳
- ۳-۷ کدبرداری GS و قضایای مربوط به آن ..... ۲۰۴
- ۱-۳-۷ مرحله درونیابی ..... ۲۰۴
- ۲-۳-۷ مرحله فاکتورگیری ..... ۲۰۵
- ۳-۳-۷ انتخاب کلمه پیام نهایی از بین کاندیداها ..... ۲۰۵
- ۴-۳-۷ روش کدبرداری  $GS(1)$  ..... ۲۰۶
- ۵-۳-۷ روش کدبردار  $GS(m)$  ..... ۲۰۸
- ۴-۷ ارائه الگوریتم‌های عملی برای کدبرداری GS ..... ۲۱۰
- ۱-۴-۷ الگوریتم‌های درونیابی ..... ۲۱۰
- ۲-۴-۷ درونیابی با یافتن ستون‌های وابسته خطی: الگوریتم Feng-Tzeng ..... ۲۱۱
- ۳-۴-۷ درونیابی با الگوریتم Kotter ..... ۲۱۸
- ۴-۴-۷ الگوریتمی برای مرحله‌ی فاکتورگیری: الگوریتم راث-راکنشتاین ..... ۲۲۴
- ۵-۴-۷ کلمات کد موجود در لیست چه باید کرد؟ ..... ۲۳۰
- ۵-۷ کدبرداری نرم کدهای RS ..... ۲۳۲
- ۶-۷ تمرین‌های فصل هفتم ..... ۲۳۷

۲۴۱	فصل هشتم: کدهای آزمون توازن کم چگالی
۲۴۳	۱-۸ تعریف کدهای آزمون توازن کم چگالی
۲۴۴	۲-۸ نمایش گرافی کدهای آزمون توازن کم چگالی
۲۴۵	۳-۸ انواع کدهای آزمون توازن کم چگالی
۲۴۶	۱-۳-۸ کدهای LDPC منظم یا کدهای گالاگر
۲۴۶	۲-۳-۸ کدهای LDPC نامنظم
۲۴۹	۴-۸ الگوریتم کدگذاری
۲۵۰	۵-۸ کدبرداری
۲۵۱	۱-۵-۸ مرحله‌ی مقداردهی اولیه
۲۵۳	۲-۵-۸ مرحله‌ی افقی
۲۵۵	۳-۵-۸ مرحله‌ی عمودی
۲۵۶	۴-۵-۸ مرحله‌ی نهایی
۲۵۷	۶-۸ تحلیل و طراحی کدهای LDPC به روش تکامل چگالی
۲۶۰	۷-۸ طراحی کد LDPC برای طول کوتاه
۲۶۱	۱-۷-۸ یافتن تنوع درجه اولیه
۲۶۲	۲-۷-۸ طراحی و بهینه‌سازی اولیه با استفاده از آستانه مجانبی
۲۶۹	۳-۷-۸ شبیه‌سازی کدهای دارای بیشترین آستانه مجانبی و انتخاب بهترین
۲۷۲	۸-۸ مقایسه کدهای بهینه در نرخ‌های مختلف
۲۷۲	۹-۸ ارزیابی عملکرد کدهای طراحی شده در مقایسه با کدهای منظم بهینه
۲۷۶	۱۰-۸ تمرین‌های فصل هشتم
۲۷۸	واژه نامه
۲۸۰	مراجع