کدهای چرخشی:

اگر C یک کد خطی باشد که روی میدان $GF(q^n)$ با طول n باشد، کد C را کد چرخشی می گویند هرگاه برای هر کلمه $(C_0, C_1, \dots, C_{n-2}, C_{n-1})$، کلمه $(C_{n-1}, C_0, \dots, C_{n-3}, C_{n-2})$ در میدان $GF(q^n)$ یک کلمه کد باشد. که این کلمه کد شیفت یافته کلمه کد قبلی است . یعنی اگر V یک کلمه کد بصورت زیر باشد:

$$V = (v_0, v_1, \dots, v_{0n-2}, v_{n-1})$$

آنگاه i بار شیفت یافته آن بصورت زیر است و یک کلمه کد محسوب می شود.

$$V^{(1)} = (v_{n-1}, v_0, \dots, v_{n-3}, v_{n-2})$$

$$V^{(i)} = (v_{n-i}, v_{n-i+1}, \dots, v_{n-i-2}, v_{n-i-1})$$

کدهای چرخشی را می توان طور دیگری نیز تعریف کرد و این واقعیت از این ناشی شده است که اگر $g(x)$ چند جمله ای مولد یک کد خطی باشد آنگاه هر ضریبی از $g(x)$ نیز یک کلمه کد است مثلا برای یک کد (n, k) داریم:

$$V(X) = v_0 + v_1X + v_2X^2 + \cdots + v_{n-1}X^{n-1}$$

$$V^{(i)}(X) = v_{n-i} + v_{n-i+1}X + v_{n-i+2}X^2 + \cdots + v_{n-i-1}X^{n-1}$$

و اگر چند جمله ای v(x) را در X^i ضرب کنیم داریم:

$$X^iV(X) = v_0X^i + v_1X^{i+1} + v_2X^2 + \cdots + v_{n-1}X^{n+i-1}$$

که آن را می توان به صورت زیر نوشت:

$$\begin{aligned} X^iV(X) = &\left[v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1} + v_0X^i \dots + v_{n-i-1}X^{n-1}\right] \\ &+ \left[v_{n-i}(X^n + 1) + v_{n-i+1}X(X^n + 1) + \cdots + v_{n-1}X^{i-1}(X^n + 1)\right] \\ &= q(x)(X^n + 1) + V^{(i)}(X) \end{aligned}$$

کد چرخشی BCH :

کدهای BCH زیر گروهی از کدهای گردشی هستند که به صورت مستقل توسط بوس، ری-چودری(۱۹۶۰) و هوکنگام(۱۹۵۹) معرفی شدند. این کدها دارای یک ساختار جبری غنی هستند که طراحی الگوریتم های کد برداری جبری کارآمد را برای آنها ممکن می سازد. این کدها هر دو نوع الفبای دودویی و غیر دودویی را در بر می گیرند. از مزیت های دیگر این کد اینست که مطالعات زیادی روی این د انجام شده است .و این کدها

برای گستره ی وسیعی از n و k ها موجود بوده و در جداولی ارائه شده اند. همچنین کدهای bch جزو شناخته تریت کدها برای طول n های کوتاه تا متوسط است.

این کدها دارای فاصله همینگ زیاد است و جز, الگوریتم های جبری تصحیح خطای بسیار مفید محسوب می شود. در این روش هر کلمه کد مضربی از چند جمله‌ای مولد است. وجود $qn - m$ کد واژه در یک کد چند جمله‌ای روی $GF(q^n)$ ، با طول کد n و چند جمله‌ای مولد $q(x)$ از ویژگی‌های این نوع کدگذاری محسوب می شود. در رمزگشایی، تشخیص خطا از طریق تقسیم چند جمله‌ای بر چند جمله‌ای مولد (باقیماندهٔ غیر صفر) صورت می گیرد، حد اقل فاصلهٔ همینگ نیز باحداقل وزن کد واژه‌های غیر صفر آن برابری می‌کند.

همانطور که گفته شده این کدها برای n های متوسط و کوتاه کارآمد است. بطور کلی با افزایش n نرخ $d_{\min}/n$ کاهش می یابد. در واقع برای تمام کدهای BCH با نرخ ثابت با افزایش n، نرخ خطاهای قابل تصتیح به سمت صفر می رود. و این نشان می دهد که کدهای BCH به طور مجانبی دهای بدی هستند

کدهای RS

کدهای رید-سولمون(RS) تقریبا رایج ترین کدهای مورد استفاده در عمل هستند این روش توسط ایروینگ اس رید و گوستاو سولومون در سال ۱۹۶۰ ابداع شد، این نوع کدگذاری تنها روش غیربایتری در بین کدگذاری‌ها محسوب می‌شود. کدگذاری ریدسالامان روشی سیستماتیک برای ساختن کدهایی با قابلیت شناسایی چندین خطای تصادفی است که توانایی تشخیص هر ترکیب از t بیت خطادار و تصحیح t/2 تا بیت را دارا است. کدگذاری رید سالامان برای استفاده به صورت تصحیح خطای بیتی مسلسل‌وار مناسب است. بیت‌های منبع به صورت ضرایب یک چندجمله‌ای p(x) بر روی یک طول محدود قرار دارند و n بیت کد از k بیت منبع با استفاده از فرانمونه‌برداری p(x) در n > k نقطه متفاوت تولید می‌شود. کدهای RS به صورت کد BCH دوره‌ای است که بیت‌های رمزکننده از روی ضرایب یک چندجمله‌ای به دست می‌آید که با استفاده از حاصلضرب p(x) و یک چندجمله‌ای مولد دوره‌ای ساخته می‌شود. این کار به یک الگوریتم رمزگشایی موثر منجر می‌شود که توسط Elwyn Berlekampو James Massey کشف شد و به الگوریتم رمزگشایی Berlekamp-Massey معروف است.

تصحیح خطای رید-سالامون

در تئوری کد، کدهای Reed–Solomon یا به اختصار (RS) در واقع کدهای غیردودویی هستند که بیت ورودی از نوع مجموعه ای بزرگتر از ۲ هستند. کدهای تصحیح خطا دایره ای توسط ایروینگ اس رید و گوستاو سولومون اختراع شد. آن‌ها یک روش سیستماتیک برای ساختن کدهایی که می‌توانند چندین خطای نشانه تصادفی توصیف کردند. با اضافه کردن t نشانه بررسی به داده، یک کد RS می‌تواند هر ترکیب از t نشانه خطادار را تشخیص دهد، و تا t/2 نشانه را تصحیح کند. به عنوان یک کد قابل حذف شدن، میتواند تا t نشانه قابل پاک شدن را تصحیح کند، یا به نوعی می توان گفت که می تواند ترکیبی از خطاها و کدهای قابل پاک شدن را تشخیص و تصحیح کند.

به علاوه، از آنجا که توالی b+1 خطای بیتی می‌تواند حداکثر دو نشانه با اندازه b را تحت تاثیر قرار دهد، کدهای RS برای استفاده به صورت تصحیح خطای بیتی مسلسل‌وار مناسب است. انتخاب t بستگی به طراح کد دارد، و می تواند در محدوده عریضی انتخاب شود.

در کدکردن رید-سالامون، نشانه‌های منبع به صورت ضرایب یک چندجمله‌ای p(x) بر روی یک طول محدود تعریف می‌شود. ایده اصلی تولید n نشانه کد از k نشانه منبع با استفاده ازفرانمونه‌برداری p(x) در n > k نقظه متفاوت، فرستادن نقطه‌های نمونه‌برداری شده، و استفاده از تکنیک میانیابی در گیرنده برای بازسازی پیام اصلی است. امروزه کدهای RS بدین روش مورد استفاده قرار نمی‌گیرند. در عوض، کدهای RS به صورت کد BCHدوره‌ای، که نشانه‌های رمزکننده از روی ضرایب یک چندجمله‌ای که با استفاده از جاصلضرب p(x) و یک چندجمله‌ای مولد دوره‌ای ساخته می‌شود بدست می‌آید.

این کار به یک الگوریتم رمزگشایی موثر منجر می‌شود، که توسط Elwyn Berlekamp و James Massey کشف شد، و به الگوریتم رمزگشایی Berlekamp-Massey معروف است. توابع code و decode به صورت مجزا تعریف شده اند