расстоянием между всевозможными словами $X'=(x'_1, \ldots, x'_l)$ и $X''=(x''_1, \ldots, x''_l)$ кода. Для того чтобы код обнаруживал все комбинации из s ошибок и исправлял все комбинации из t ошибок, необходимо и достаточно, чтобы кодовое расстояние было равно $s+t+1$.

Широкий класс кодов для симметричного канала составляют линейные (групповые) коды [3], напр. коды Хэммйнга, широко применяющиеся для защиты информации в основной памяти ЭВМ. Код Хэмминга обладает кодовым расстоянием $d=3$, исправляет однократные ошибки и обнаруживает двукратные. Он имеет проверочные разряды, расположенные в позициях с номерами 2^0, 2, 2^2, . . . Линейный код задаётся парой матриц: порождающей $G_{n\times l}=\|\overline{g_j}\|$, $j=\overline{1,n}$, и проверочной $H_{k\times l}$. Строки g_j порождающей матрицы — линейно независимые векторы, образующие базис пространства, содержащего 2^n элементов — кодовых слов. Каждая из строк проверочной матрицы ортогональна строкам $\overline{g_j}$, $j=\overline{1,n}$, и $GH^T=0$.

Кодер линейного кода образует кодовые слова по правилу $X^T=U^TG$. Модель искажений предполагает, что в канале с X посимвольно суммируется шумовой вектор Z, образуя слово $Y=X+Z$.

Идея декодирования заключается в образовании произведения $S^T=Y^TH^T$, называемого с и н д р о м о м. Равенство $S=0$ означает, что $Z=0$, либо ошибка относится к необнаруживаемым. Синдром имеет 2^k-1 ненулевых реализаций, каждая из к-рых может быть использована для указания на произошедшую ошибку.

Циклич. коды входят как подкласс в групповые коды. В них вместе со словом X входят и все его циклич. перестановки. Кодовые слова образуются как произведение двух полиномов: $U(E)$ степени $n-1$, коэф. к-рого составляют информационное слово U, и порождающего $g(E)$ степени $l=n$, неприводимого и делящего без остатка двучлен $(1+E^l)$. Декодирование заключается в делении принятого слова (полинома) на $g(E)$. Наличие ненулевого остатка укажет на присутствие ошибки. Циклич. коды, как правило, несистематические.

Спец. циклич. коды предназначены для обнаружения и исправления пачек ошибок, напр. коды Файра, определяемые порождающими полиномами вида $g(E)=p(E)(E^c+1)$, где $p(E)$ — неприводимый полином, а величина c определяется длиной исправляемых и обнаруживаемых пачек ошибок.

Пачки ошибок характерны для запоминающих устройств с магн. носителями, в частности для накопителей на магн. дисках (НМД) совр. ЭВМ (см. *Памяти устройства*). Для защиты данных в НМД поэтому широко используется К. и. циклич. кодами, осуществляемое аппаратными средствами.

Арифметические коды предназначены для обнаружения ошибок, возникших при выполнении арифметич. операций на ЭВМ. В теории арифметич. кодирования вводятся понятия веса, расстояния и ошибки, отличные от хэмминговых. Арифметич. вес числа определяется как мин. число слагаемых в представлении числа в виде $N=\sum_i a_i 2^{j_i}$, $a_i \in (1, -1)$. Ошибки, в результате к-рых величина числа изменяется на $\pm 2^i$, $i=0, 1, 2, \ldots$, наз. арифметическими. Арифметич. расстояние между N_1 и N_2 — арифметич. вес разности $(|N_1-N_2|)$, равно кратности ошибки, переводящей число N_1 в N_2, и определяет корректирующую способность арифметич. кода подобно расстоянию Хэмминга.

В распространённых AN-кодах кодирование числа N — операнда — осуществляется умножением его на специально подобранный множитель A. Так, 3A-код, имея кодовое расстояние 2, обнаруживает одиночные ошибки путём деления суммы на 3. Ошибки обнаруживаются при ненулевом остатке: величина арифметич. ошибки 2^i не делится на 3 нацело. Кроме одиночных при $A=3$ обнаруживается и часть двойных ошибок — те, при к-рых правильный и ошибочный результат имеет несовпадающие остатки от деления на 3.

Криптография осуществляется путём подстановки, когда каждой букве шифруемого сообщения ставится в соответствие определ. символ (напр., др. буква), либо путём перестановки, когда буквы внутри искусственных блоков текста меняются местами, либо комбинацией этих методов. Шенноном показано, что возможны криптограммы, не поддающиеся расшифровке за приемлемое время [5].

Лит.: 1) Стахов А. П., Введение в алгоритмическую теорию измерения, М., 1977; его же, Коды золотой пропорции, М., 1984; 2) Акушский И., Юдицкий Д., Машинная арифметика в остаточных классах, М., 1968; 3) Галлагер Р., Теория информации и надежная связь, пер. с англ., М., 1974; 4) Дадаев Ю. Г., Теория арифметических кодов, М., 1981; 5) Аршинов М. Н., Садовский Л. Е., Коды и математика, М., 1983. *А. Н. Ефимов.*

КОЛЕБА́НИЯ — движения или состояния, обладающие той или иной степенью повторяемости во времени. К. свойственны всем явлениям природы: пульсирует излучение звёзд, внутри к-рых происходят циклич. ядерные реакции; с высокой степенью периодичности вращаются планеты Солнечной системы (а всякое вращение можно представить себе как два одновременных К. во взаимно перпендикулярных направлениях); движение Луны вызывает приливы и отливы на Земле; в земной ионосфере и атмосфере циркулируют потоки заряж. и нейтральных частиц; ветры возбуждают К. и волны на поверхностях водоёмов и т. д. Внутри любого живого организма — от одиночной клетки до высокоорганизованных их популяций — непрерывно происходят разнообразные, ритмично повторяющиеся процессы (биение сердца, колебания психич. состояний и др.). В виде сложнейшей совокупности К. частиц и полей (электронов, фотонов, протонов и др.) можно представить «устройство» микромира.

В технике К. выполняют либо определ. функциональные обязанности (колесо, маятник, колебат. контур, генератор К. и т. д.), либо возникают как неизбежное проявление физ. свойств (вибрации машин и сооружений, неустойчивости и вихревые потоки при движении тел в газах и т. д.).

В физике особо выделяются колебания двух видов — механич. и электромагнитные и их эл.-механич. комбинации. Это обусловлено той исключит. ролью, к-рую играют гравитац. и эл.-магн. взаимодействия в масштабах, характерных для жизнедеятельности человека. С помощью распространяющихся механич. К. плотности и давления воздуха, воспринимаемых нами как звук, а также очень быстрых колебаний электрич. и магн. полей, воспринимаемых нами как свет, мы получаем бо́льшую часть прямой информации об окружающем мире.

К. любых физ. величин почти всегда сопровождаются попеременным превращением энергии одного вида в энергию другого вида. Так, оттягивая маятник (груз на нити) от положения равновесия, мы увеличиваем потенц. энергию груза, запасённую в поле тяжести; при отпускании он начинает падать, вращаясь около точки подвеса как около центра, и в крайнем ниж. положении вся потенц. энергия превращается в кинетическую, поэтому груз проскакивает это равновесное положение, и процесс перекачки энергии повторяется, пока рассеяние (диссипация) энергии, обусловленное, напр., трением, не приведёт к полному прекращению К. В случае К. электрич. зарядов и токов в *колебательном контуре* или электрич. и магн. полей в эл.-магн. волнах роль потенциальной обычно играет электрич. энергия, а кинетической — магнитная. Иногда, когда речь идёт о К. тепловых, хим. и особенно информац. величин, такой энергетич. подход несколько условен, но вполне плодотворен.

Т е о р и я к о л е б а н и й и в о л н. Изучение К. на разных этапах играло стимулирующую роль в развитии науки. Так, исследования К. маятника