УДК 519.48

К теории самодвойственных полиномов над полем Галуа. Р. Р Варшамов, Г. А. Гараков. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 5—17.

В статье дается описание важнейших специфических свойств самодвойственных полиномов. На основании полученных результатов выводится конечная формула общего числа неприводимых в поле $GF(q)$ нормированных самодвойственных полиномов степени m. Кроме того, исследуется одно квадратичное преобразование, играющее важную роль в теории синтеза неприводимых самодвойственных полиномов.

Табл. нет, рис. нет, библиографий 2.

УДК 51:621.391

Некоторые свойства рекуррентных периодических последовательностей В. А. Аракелов, Г. М. Тененгольц. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 18—28.

Работа состоит из трех параграфов. В § 1 рассматривается множество m вычетов выражения x^N (целое $N \geqslant 0$) по модулю полинома $h(x) = x^n + x^m + 1$ с коэффициентами из поля $GF(2)$. Легко видеть, что для всякого целого $N \geqslant 0$ имеет место сравнение:

$$x^N \equiv \varphi_0(N) + \varphi_1(N)\,x + \cdots + \varphi_{n-1}(N)\,x^{n-1} \pmod{h(x)},$$

где коэффициенты $\varphi_l(N) \in GF(2)$. Предлагается метод, позволяющий по заданным коэффициентам φ за число шагов $e < n$ определить величину N.

В § 2 для функции $T(n_1, n_2 \cdots n_l)$ [$T(n_1, n_2, \cdots n_l)$ — показатель, которому принадлежит полином $h(x) = x^{n_1} + x^{n_2} + \cdots + x^n t + 1$ над полем $GF(2)$], выводятся следующие справедливые для любых целых положительных t и k соотношения:

$$1)\ T(2^k, 1) = 2^{2k} - 1.$$

$$2)\ T\left(\frac{2^{tk}-1}{2^k-1},\ \frac{2^{(t-1)k}-1}{2^k-1},\ \cdots 1\right) = 2^k\left(\frac{2^{tk}-1}{2^k-1}\right) + 1.$$

В последнем параграфе исследуются некоторые взаимосвязи между корнями неприводимых полиномов $f(x)$ и $f(1+x)$, позволяющие строить ортогональные соотношения размера два. Табл. нет, рис. нет, библиографий 3.

УДК 51:621.391

О некоторых вопросах декодирования линейных кодов. Р. Д. Петросян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 29—34.

Рассматривается двоичный (n, k)-код максимальной длины. Описывается очень простой алгоритм, позволяющий путем несложных подсчетов определить принадлежность произвольного синдрома $z \in Z$ к одному из непересекающихся подмножеств $z_1, z_2, \cdots z_k$, на которые разбивается множество Z всевозможных синдромов, при условии, что при передаче по каналу связи проверочная часть кодового слова не подвергается искажениям.

Решение задачи сводится к определению j, $j = 1, 2, \cdots k$, при котором значение некоторой функции $\Delta_{i,j}(z)$, характеризующей „близость" $z \in z_i$ к z_j, достигает максимума.

Выводится формула, дающая значение $\Delta_{i,j}(z)$ при данных i и j.

Табл. нет, рис. нет, библиографий нет.

УДК 51:621.391

Нахождение циклических представителей в бинарных циклических алфавитах. С. Ш. Оганесян, В. Г. Ягджян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 35—38.

Рассматривается задача нахождения весового спектра циклических кодов для исследования их корректирующих возможностей. Приведен метод нахождения циклических представителей, который облегчает вычисление спектра.

Табл. нет, рис. нет, библиографий 2.

УДК 51:621.391

Объединение циклических представителей по одинаковым весам в бинарных алфавитах. С. Ш. Оганесян, В. Г. Ягджян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 39—48.

Рассматривается задача объединения циклических представителей в квадратичные представители, которые существенно сокращают машинное время для исследования корректирующих возможностей циклических алфавитов. Доказана основная теорема о нахождении квадратичных представителей алфавитов, являющихся объединением двух минимальных идеалов, которую легко обобщить для более общих алфавитов при соответствующих ограничениях.

Табл. нет, рис. нет, библиографий 1.

УДК 51:621.391

О пороговом декодировании циклических кодов Хемминга. И. М. Бокриков „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 49—53.

В статье доказывается невозможность полной ортогональности кодов Хемминга. Предлагается модифицированный метод порогового декодирования, позволяющий исправлять одиночную ошибку. Метод применяется также и в исправлении стирания двух символов и одиночных пачек ошибок длины 2.

Табл. нет, рис. нет, библиографий 3.

УДК 51:621.391

Класс кодов, исправляющий две несимметричные ошибки. Р. Р. Варшамов, Э. П. Зограбян. „Математические вопросы кибернетики и вычислительной техники", 1970 г., VI, стр. 54—58.

Рассматривается множество $G_{n,q}$ — всевозможных последовательностей вида $x = (x_1\ x_2, \cdots, x_n)$, где каждый знак x_i принимает одно из значений 0, 1, $\cdots, q-1$ (где q произвольное целое $\geqslant 2$). в $G_{n,q}$ вводится понятие нормы $|x|$ как суммы элементов, входящих в последовательность x, т. е. $|x| = \sum_{i=1}^{n} x_i$. Под r-кратным несимметричным искажением сигнала x понимается обычное сложение его с вектором $y \in G_{n,q}$ ($|y| \leqslant r$), удовлетворяющим одному из условий

$$|x + y| = |x| + |y|$$

или

$$|x - y| = |x| - |y|.$$

Показывается, что множество $H_{\alpha,\beta} \in G_{n,q}$ — всевозможных решений системы сравнений

$$\sum_{i=1}^{n} i x_i \equiv \alpha \pmod{p-1}$$

$$\sum_{i=1}^{n} (q^i - 1)\, x_{i_1} \equiv \beta \pmod{p}$$

(где α и β—произвольные целые, $p > 5$ — простое число, q — первообразный корень по модулю p, $n < p - 1$) является кодом, исправляющим все одиночные и двойные несимметричные ошибки. В конце статьи утверждается, что множество $\overline{H}_{\alpha,\beta} \in G_{n,q}$ — всевозможных решений системы сравнений

$$\sum_{i=1}^{n} i x_i \equiv \alpha \pmod{p}$$

$$\sum_{i=1}^{n} i^2 x_i \equiv \beta \pmod{p}$$

также является кодом, исправляющим две несимметричные ошибки.

Табл. нет, рис. нет, библиографий 2.

УДК 51:621.391

Об одной общей схеме декодирования циклических кодов. Р. Д. Петросян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 59—63.

Рассматривается весьма эффективная общая схема декодирования двоичных циклических (n, k)-кодов (допускающая обобщение и на случай недвоичных циклических кодов) при любом из следующих условий:

а) число исправляемых ошибок $r \leqslant 3$, k — любое,

б) число информационных символов $k \leqslant 5$, r — любое.

Исправление ошибок производится исходя из показаний счетчиков, регистрирующих число совпадений между компонентами проверочного вектора, определяемого по принятому кодовому слову, и проверочными символами каждого из кодовых слов, содержащих среди информационных символов лишь одну единицу. При этом используется равенство значений j-ых проверочных символов этих слов коэффициентами j-го проверочного соотношения (т. е. проверочного соотношения для j-го проверочного символа). Показывается, что техническая реализация устройства для получения коэффициентов проверочных соотношений по сложности идентична кодирующему устройству.

Декодирование осуществляется параллельно с вычислением компонент проверочного вектора, благодаря чему не требуется повышения скорости обработки информации.

Табл. нет, рис. 4, библиографий 1.

УДК 51:621.391

Некоторые классы корректирующих кодов. В. А. Аракелов, Г. М. Тененгольц. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 64—77.

В работе для построения кодов длины n с произвольным основанием $q > 2$, устойчивых к одиночным сбоям типа вставок или выпадений, а также к одиночным несимметрическим искажениям, используется сравнение

$$W = \sum_{i=1}^{n} i\beta(z_i) \equiv a \pmod{m}, \qquad (1)$$

где

$$\beta(z_i) = \sum_{t=0}^{z_i-1} n^t, \quad z_i = 0, 1, 2 \cdots q-1,$$

a — произвольное целое, $m = \sum_{v=0}^{q-1} n^v$.

Для некоторых частных случаев сравнения (1) строится оптимальный, в данном классе, код, исправляющий одиночные симметрические ошибки. В бинарном случае указанные коды рассматриваются как систематические и используются для построения универсальной системы кодирования с исправлением одиночных несимметрических (симметрических) ошибок или ошибок типа вставок (выпадений).

Табл. нет, рис. 4, библиографий 6.

УДК 51:621.391

О реализации алгоритма синтеза линейных кодов. Э. П. Зограбян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 78—87.

Описывается алгоритм синтеза линейных кодов для дискретной системы связи с произвольной статистической структурой источника шумов. Рассматриваются два метода реализации алгоритма на специализированном программно-управляемом устройстве. Для одного из методов приводится расчет математического ожидания времени реализации.

Табл. 1, рис. 2, библиографий 2.

УДК 51:621.391

Об одном методе построения линейных кодов. Э. П. Зограбян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 88—92.

Уточняется граница избыточности линейных кодов, допускающих исправления ошибок, порождаемых заданным множеством канальных помех из достаточно широкого класса множеств помех. Описывается метод построения проверочной матрицы для указанных кодов. Доказывается, что в некотором подклассе множеств помех построенные описанным методом коды являются оптимальными.

Табл. нет, рис. нет, библиографий 2.

УДК 519.24

Об одной задаче различения двух сигналов. Д. Г. Асатрян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 93—104.

Рассматривается следующая задача выбора решения. В соответствии с некоторым законом λ порождается бинарная последовательность сигналов, длина которой N. В канале связи на каждый сигнал независимо накладывается стационарный аддитивный шум с нулевым средним. При условии, что наблюдателю известны некоторые свойства закона λ, требуется построить правило решения относительно каждого члена последовательности сигналов, качество работы которого определяется средним числом элементов последовательности, где решение было ошибочным.

Если сигналы порождаются независимо друг от друга, то нетрудно указать оптимальное пороговое правило обработки принятой реализации, в смысле выбранного критерия (байесовское правило). Если же закон λ таков, что существует в определенном смысле связь между соседними сигналами, то целесообразно использовать другое правило выбора решения, которое минимизирует „неупорядоченность" появления сигналов. Исследуются некоторые свойства указанного решающего правила и находится класс законов λ, в котором оно равномерно лучше байесовского правила.

Табл. нет, рис. нет, библиографий 2.

УДК 681.3

Усовершенствование метода построения делительных устройств. Д. О. Мелконян. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 105—111.

Статья посвящена вопросу построения оптимального по быстродействию и затратам оборудования делительного устройства.

Вначале статьи рассматриваются классические схемы для производства непосредственного деления „П"-разрядных двоичных чисел и приведены их параметры по быстродействию и экономичности. Сравнивая их, автор приходит к выводу: сравнительная экономичность одной схемы обесценивается ее невысоким быстродействием, сравнительно же высокое быстродействие другой схемы, наоборот, обесценивается ее неэкономичностью.

Далее приводится предлагаемый автором метод построения делительного устройства. Метод основан на использовании регистра с кольцевым сдвигом и сумматора с кольцевым переносом и обеспечивает сочетание экономичности первой классической схемы с быстродействием второй.

В заключение автор указывает возможность объединения в одном блоке делительного и множительного устройства. Последнее выполняется в соответствии с методом, изложенным в статье „Метод ускоренного точного умножения двоичных чисел в цифровой вычислительной машине" (журнал „Приборостроение" № 2, 1962).

Табл. нет, рис. 2, библиографий нет.

УДК 519.48

Таблицы неприводимых полиномов над полем GF(p) ($p < 11$). Г. А. Гараков. „Математические вопросы кибернетики и вычислительной техники". 1970 г., VI, стр. 112—142.

Приводятся таблицы нормированных неприводимых полиномов для первых пяти простых модулей, полученные на ЭЦВМ „Раздан-3" по разработанному автором алгоритму.

Указанные таблицы по объему значительно превосходят известные в настоящее время в литературе таблицы подобного рода.

Табл. 1, рис. нет, библиографий 4.