ИДЕЯ ЗА ТЕОРИЯ НА КОДИРАНЕТО
– ЗА МАТЕМАТИЦИ И НЕМАТЕМАТИЦИ

Веселин Дренски
Институт по математика и информатика – БАН
e-mail: drensky@math.bas.bg

Семинар на тема
„Велико Търново – наука, духовност, развитие“,
посветен на 70-годишнината
от рождението на акад. Стефан Додунеков
(Велико Търново, 11 септември 2015 г.)

Частично финансирано от Договор И02/18 с Фонд „Научни изследвания“.

В памет на акад. Стефан Додунеков

(05.09.1945 – 05.08.2012)

Началото на историята на този доклад започва преди около 30 години, когато ми попадна една прекрасна популярна статия за теория на кодирането, написана от френския математик Жак Волфман от Университета в Тулон:

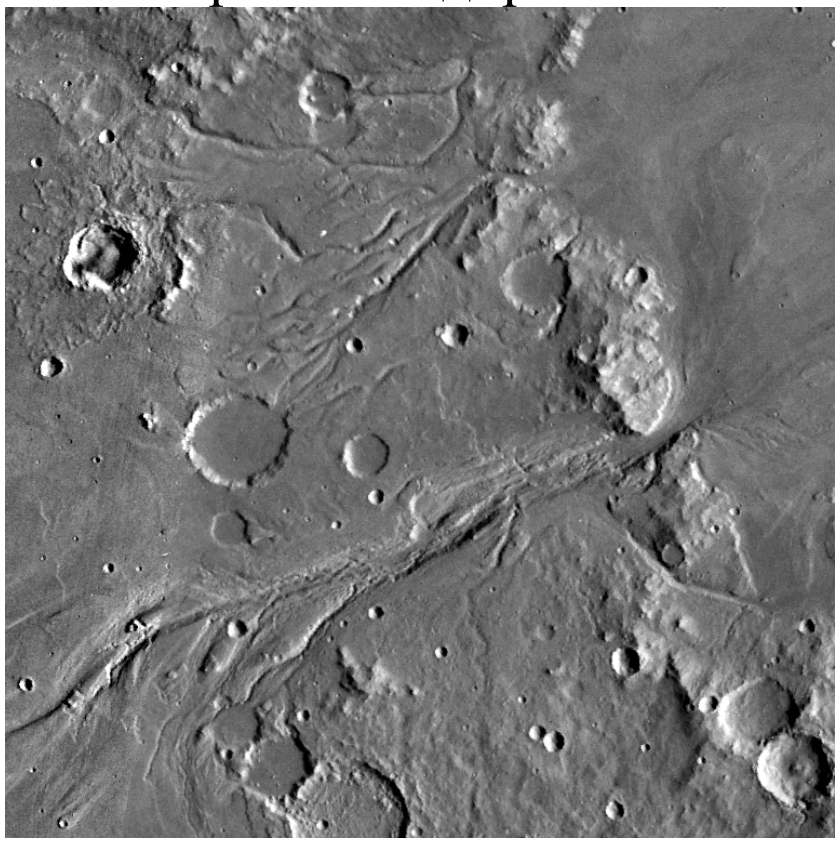
J. Wolfmann, Évariste Galois et la planète Mars:
Introduction à la théorie algébrique du codage,
Colloque d algèbre (Univ. de Rennes I, 20 au 24 Mai 1985).
Publ. Inst. rech. math. Rennes, fasc. IV, Algèbre (1986),
123-147.

Обяснения към заглавието:

Еварист Галоа – гениален френски математик,

загинал само на 21 години, поставил началото на теорията на Галоа, която решава въпроса кога едно алгебрично уравнение има решение в радикали с методи, които поставят началото на съвременната алгебра и са много далече от алгебричните уравнения. В негова чест крайните полета, които са абстрактни алгебрични обекти и са в основата на теорията на кодирането, са наречени полета на Галоа.

Планетата Марс – по това време, през 1985 г., все още е жив споменът за фотографиите на Марс, получени от Маринър 9, високото качество на които се дължи на използването на теория на кодирането.



Когато показах статията на Стефан Додунеков, той ми предложи да я преведа за „жълтото списание“. По това време така наричахме „Физико-математическото списание“, което беше с жълта корица и което спря да излиза през 1994 г.

Жак Волфман, Еварист Галоа и планетата Марс: въведение в алгебричната теория на кодирането, Физ.-мат. списание 30(63) (1988), № 2, 104-116.

Идеи от тази статия са използвани в настоящия доклад.

Съвременната теория на кодирането започва с основополагащата статия на Шенон от 1948 г.
C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J., 27 (1948), 379-423, 623-656.

Тя възниква като опит да се реши следният
Основен проблем при предаването на информация на разстояние:
Появяване на грешки в резултат на смущения по канала.
Пример: Изпратена телеграма (за по-младите – SMS):

ЧАКАЙ ГАРАТА 11.09,16:15.

Получено (например поради грешка на телеграфиста или на изпращащия SMSa):

ЧАКАЙ ГАРАТА 12.09,16:15.

Очевиден въпрос: Какво ще стане, ако отидем да посрещнем някого на гарата с един ден закъснение?

Задача: Откриване на грешките.

Примери:

- Предаване на съобщението (или на част от него) два пъти (излишък на информация).

Изпратена телеграма:

ЧАКАЙ ГАРАТА 11.09,16:15, 11.09,16:15.

Получено:

ЧАКАЙ ГАРАТА 12.09,16:15, 11.09,16:15.

- Добавяне на контролен символ (отново излишък на информация).

  ISBN (International Standard Book Number)

  Идентификатори за България: 954 и 619.

  Иван Вазов, Под игото, 2006 г. ISBN: 9-543-40001-6

  Последната цифра е контролна (от 0 до 10, 10 = X):

  $$9 \times 10 + 5 \times 9 + 4 \times 8 + 3 \times 7 + 4 \times 6 + 0 \times 5 + 0 \times 4 + 0 \times 3 + 1 \times 2 + 6 = 220 \equiv 0 \pmod{11}$$

  С други думи: сумата от първата цифра, умножена по 10, втората – по 9, и т.н., десетата – по 1 и единадесетата цифра, се дели на 11.

- Проверка за четност:
  Обикновено в теория на кодирането се предават „двоични думи” с еднаква дължина (редички с фиксирана дължина, които се състоят от нули и единици).
  Добавя се допълнителен символ така, че разширената дума да има четен брой единици:

  $$010110 \rightarrow 0101101.$$

Задача: Коригиране на грешките. (Отново необходимост от излишък на информация).
След установяване, че има грешка, отправяне на запитване за коригирането ѝ.
Много често това е невъзможно (например при еднократно предаване на уникална информация или при липса на възможност за запитване по други причини).
Основни принципи:

- Предаването на съобщението няколко пъти:

Изпратена телеграма:

ЧАКАЙ ГАРАТА
11.09, 16:15, 11.09,16:15, 11.09,16:15.

Получено:

ЧАКАЙ ГАРАТА
12.09,16:15, 11.09,16:15, 11.09,16:15.

Чрез „гласуване” – вярната цифра е 1.

- Заменяне (кодиране) на „буквите” на съобщението с „думи”, които са достатъчно различни една от друга.
  Примери:
  В немския флот в началото на XX век
  сигналът за бедствие е SOE **(… – – – .)**.
  Тъй като последната морзова точка може да се „загуби”, сигналът е заменен с SOS **(… – – – …)**.
  В телефонни разговори:
  А като Айтос, Б като Бургас, В като Варна.
  Във ВВС на NATO и в гражданската авиация (например при купуване на самолетни билети):
  Alpha, Bravo, Charlie, Delta.
  St. John, New Brunswick = YSJ = Yankee, Sierra, Juliet
  St. John’s, Newfoundland = YYT = Yankee, Yankee, Tango

В теория на кодирането: Комбиниране на принципите за проверка на четност и достатъчно далечни една от друга думи.

Пример: Искаме да предадем съобщение, записано в азбука от 16 символа 0,1,2,...,15. В двоичен запис това са числата

0=0000, 1=0001, 2=0010, ... , 15=1111.

Работим над полето с два елемента GF(2)={0,1}, със събиране и умножение по модул 2.

За „нематематиците“: GF(2) е множество от два елемента 0 (четно) и 1 (нечетно), в което сме дефинирали „събиране“ и „умножение“ по правилата:

„четно + четно = четно“, „четно + нечетно = нечетно“,
„нечетно + нечетно = четно“,
„четно × число = четно“, „нечетно × нечетно = нечетно“

+	0	1
0	0	1
1	1	0

Таблица за събирането

×	0	1
0	0	0
1	0	1

Таблица за умножението

Елементите на нашата азбука са двоични думи с дължина 4. С цел наличие на излишък от информация, кодираме елементите на азбуката с думи с дължина 8 – елементи на 8-мерното линейно пространство

$$\mathrm{GF}(2)^8 = \{(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8) \mid a_i \in \mathrm{GF}(2)\}.$$

Разглеждаме 4-мерното подпространство C с базис

$$f_0 = (1,1,1,0,1,0,0,0),\ f_1 = (1,1,0,1,0,1,0,0),$$

$$f_2 = (1,0,1,1,0,0,1,0),\ f_3 = (1,1,1,1,1,1,1,1).$$

Това е множеството от всички суми на няколко от думите f_0, f_1, f_2, f_3 (0, 1, 2, 3 от тях или на всичките 4).

Кодиране:

Съпоставяме на числото (в двоичен запис)

$$b=2^3b_3 + 2^2b_2 + 2b_1 + b_0 = b_3b_2b_1b_0$$

елемента на C

$$f(b) = b_0f_0 + b_1f_1 + b_2f_2 + b_3f_3.$$

Елементите на C са

0 = 0 = (0,0,0,0,0,0,0,0),
1 = f_0 = (1,1,1,0,1,0,0,0),
2 = f_1 = (1,1,0,1,0,1,0,0),
3 = $f_0 + f_1$ = (0,0,1,1,1,1,0,0),
4 = f_2 = (1,0,1,1,0,0,1,0),
5 = $f_0 + f_2$ = (0,1,0,1,1,0,1,0),
6 = $f_1 + f_2$ = (0,1,0,1,1,0,1,0),
7 = $f_0 + f_1 + f_2$ = (1,0,0,0,1,1,1,0),
8 = f_3 = (1,1,1,1,1,1,1,1),
9 = $f_1 + f_3$ = (0,0,0,1,0,1,1,1),
10= $f_1 + f_3$ = (0,0,1,0,1,0,1,1),
11 = $f_0 + f_1 + f_3$ = (1,1,0,0,0,0,1,1),
12 = $f_2 + f_3$ = (0,1,0,0,1,1,0,1),
13 = $f_0 + f_2 + f_3$ = (1,0,1,0,0,1,0,1),
14 = $f_1 + f_2 + f_3$ = (1,0,1,0,0,1,0,1),
15= $f_0 + f_1 + f_2 + f_3$ = (1,0,1,0,0,1,0,1).

Свойство: Всеки два елемента на C се различават поне в 4 позиции.

Разстоянието на Хеминг между тях е ≥ 4.

Разстояние на Хеминг:
$d(u,v)$ = брой на координатите, в които се различават u и v
= брой на ненулевите координати на u – v.
Нека в нашия пример сме предали символа
10 = 1010, т.е. $f = f(1010) = f_1 + f_3 = (0,0,1,0,1,0,1,1)$
и нека до получателя е стигнало съобщението
$g = (0,1,1,0,1,0,1,1)$ с грешка във втората координата.
Разстоянието на Хеминг между g и f е 1,
а между g и всички останали думи от C е ≥ 3. По такъв начин нашият код може да коригира една грешка. Този код има параметри $[n,k,d]=[8,4,4]$.
(n = дължина на кода, k = размерност на кода,
d = минимално разстояние между кодовите думи),
Коригира $[(d-1)/2]$ грешки
(цялата част на числото $(d-1)/2$).
При $d = 4$: $(d-1)/2 = 3/2 = 1.5$, $[(d-1)/2] = 1$.

Този код е частен случай на известните кодове на Рид-Малер, открити от Малер и с предложен прост алгоритъм за декодиране от Рид през 1954 г.

Основно правило: „Добрите“ кодове имат добри алгебрични, комбинаторни и геометрични свойства.

Връзка на кодовете на Рид-Малер с алгебрата:

Разглеждаме алгебрата на полиномите GF(2)[x,y,z] на три променливи над полето с два елемента и нейната фактор алгебра

$$R = \mathrm{GF}(2)[x,y,z]/(x^2 - 1, y^2 - 1, z^2 - 1).$$

Линейното пространство R над GF(2)[x,y,z] има базис

$$1, x, y, z, xy, xz, yz, xyz.$$

С други думи, елементите на R са полиноми на x, y и z, в които всяка от променливите е от нулева или първа степен, а коефициентите са равни на 0 и 1.

Съпоставяме на елемента

$$f = b_1 + b_2x + b_3y + b_4z + b_5xy + b_6xz + b_7yz + b_8xyz$$

двоичния вектор $(b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8)$.

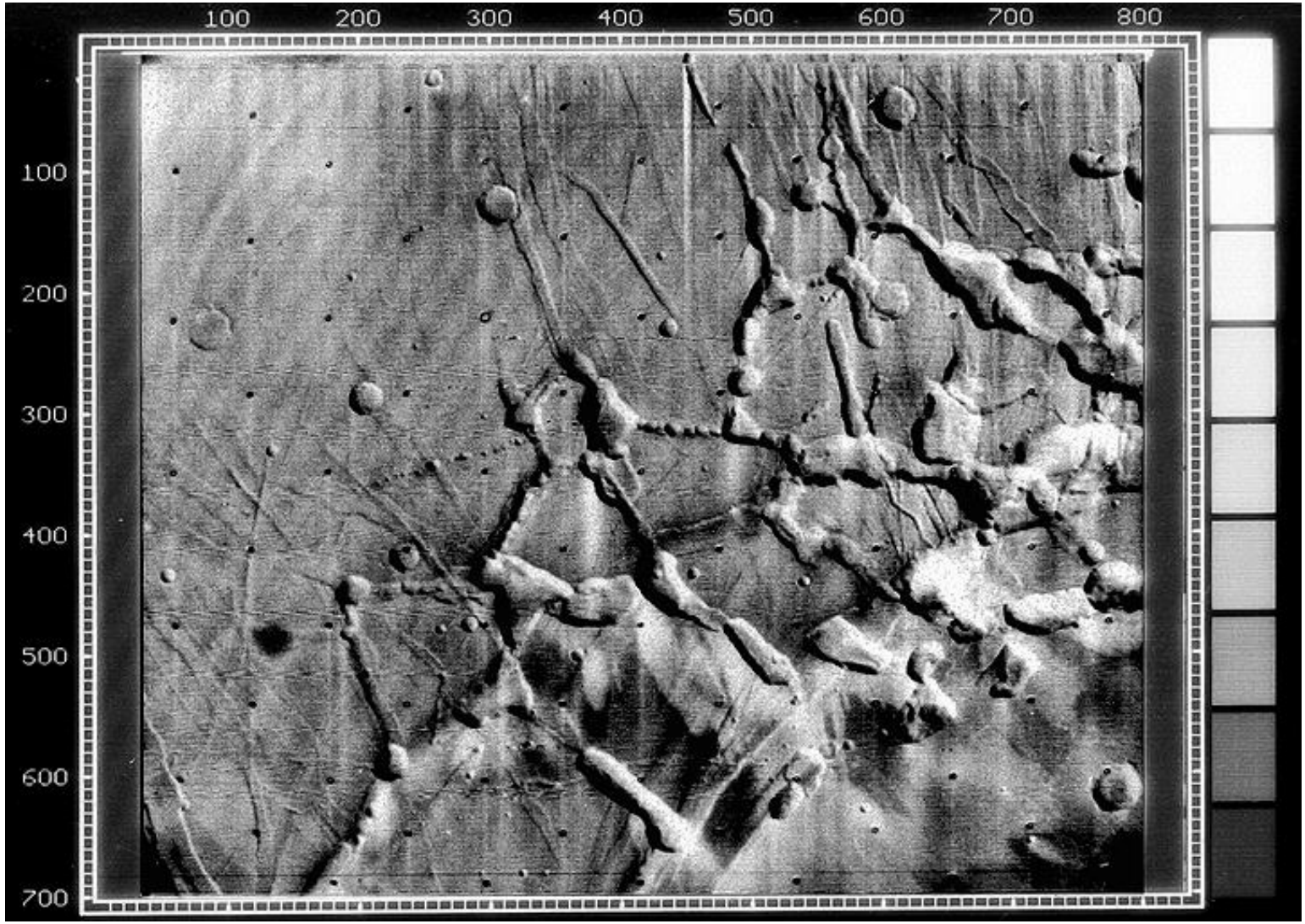
Ще отъждествяваме кода C с неговия прообраз в R. Тогава линейното пространство C има базис, състоящ се от произведенията

$$(1 - x)(1- y),\ (1 - x)(1 - z),\ (1 - y)(1 - z),$$
$$(1 - \mathrm{x})(1 - \mathrm{y})(1 - \mathrm{z}),$$

а C е идеал в R, породен от произведенията на два множителя

$$(1 - x)(1- y),\ (1 - x)(1 - z),\ (1 - y)(1 - z).$$

На 30 май 1971 г. НАСА изстрелва Маринър 9,
който на 14 ноември 1971 г. достига планетата Марс и чрез черно-бяла телевизионна камера започва да предава изображения оттам. За целта картината се разделя на малки квадратчета и на всяко квадратче се съпоставя число от 0 до 63 (в бинарен код) взависимост от степента на сиво в квадратчето.

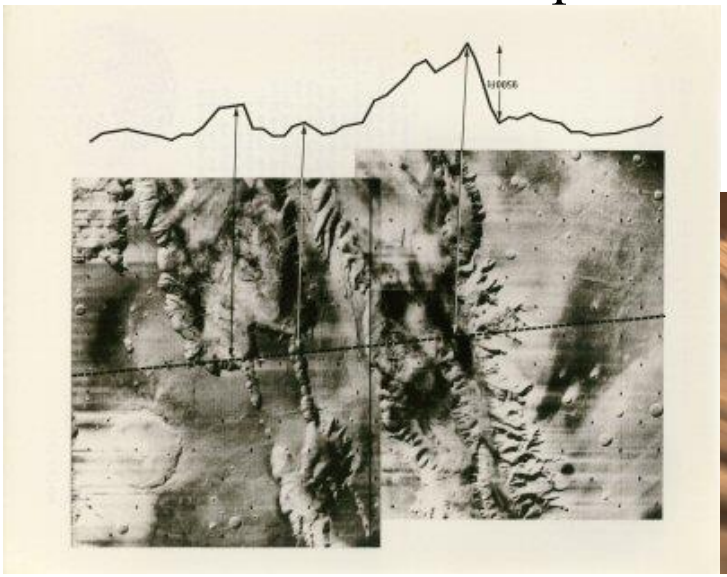

100
200
300
400
500
600
700
800
100
200
300
400
500
600
700

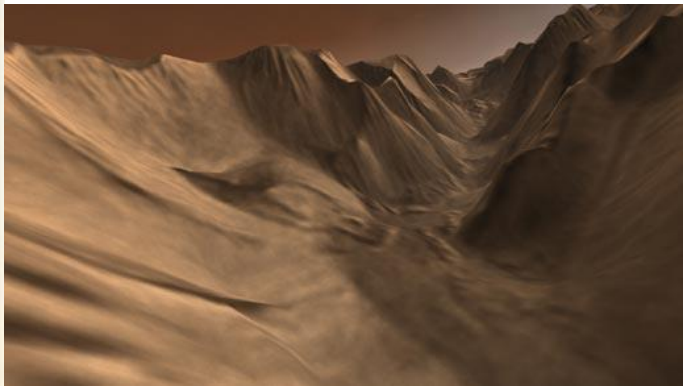
Без кодиране на сигнала, при вероятност за грешка $p = 0.05$, около 26% от образа би бил грешен, което е твърде много. Всяко кодиране увеличава дължината на кодовите думи. Поради ред технически причини се оказва, че дължината на кодовата дума не трябва да надвишава повече от 5 пъти дължината на данните, т.е. дължината на използвания код трябва да бъде около 30 бита.

Ако се използва код, който коригира 2 грешки, би се постигнала 1% грешка в образа. Ако кодът коригира до 7 грешки, грешките при образа се намаляват до 0.01%. При избора на код се оказва решаващо възможността за бързо декодиране в реално време. НАСА решава да използва код на Рид-Малер с параметри [32,6,16], който е аналогичен на разгледания по-горе. По-долу е една от снимките на Големия каньон на Марс (наречен Valles Marineris в чест на Маринър 9).

VALLES MARINERIS ON MARS (MARINER 9 / NASA)

Впоследствие, чрез наслагване на снимките (+математически и топографски методи) се пресъздава тримерно изображение на Големия каньон на Марс.





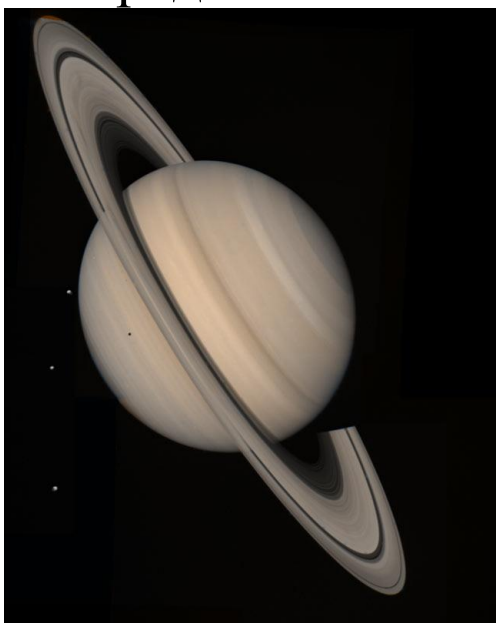
Вояджър 1 и Вояджър 2 са изстреляни съответно на 5 септември и 22 август 1977 г.

Вояджър 1

и вече 38 години продължават да предават сигнали, въпреки че са реликви от ранната космическа ера, всеки от тях с компютърна памет от 68 килобайта.

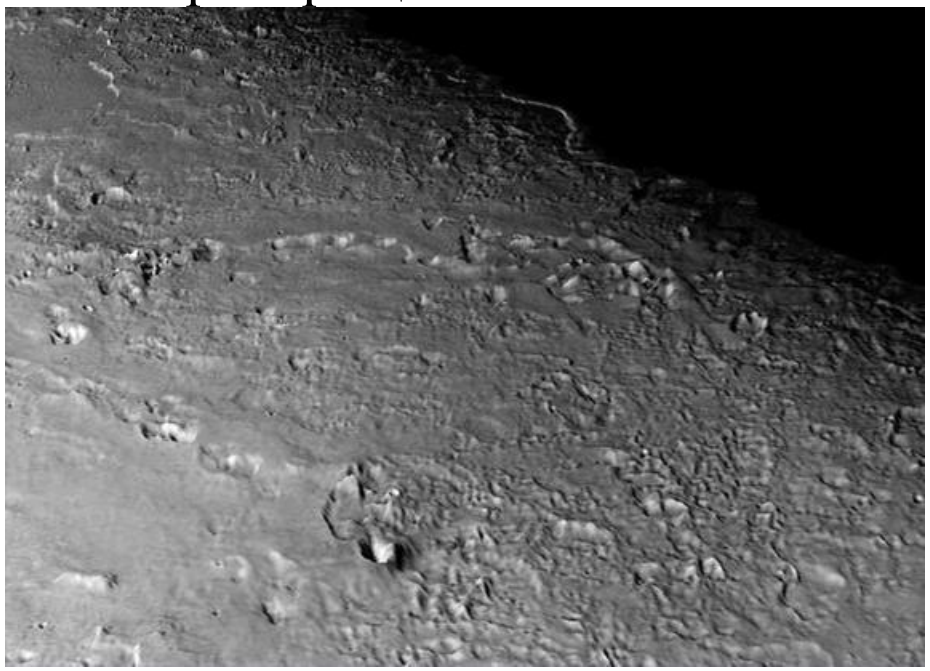
За сравнение мобилният телефон Sony Ericsson T290i (модел 2004 г., спрян от производство) е с памет 400 килобайта.

Двата Вояджъра предават цветни снимки от Юпитер и Сатурн, които изискват 3 пъти повече данни. Затова при тях се използва друг код, т.н. код на Голей с параметри [24,12,8]. Той коригира само три грешки, но е с много по-голяма скорост на предаване на информацията.



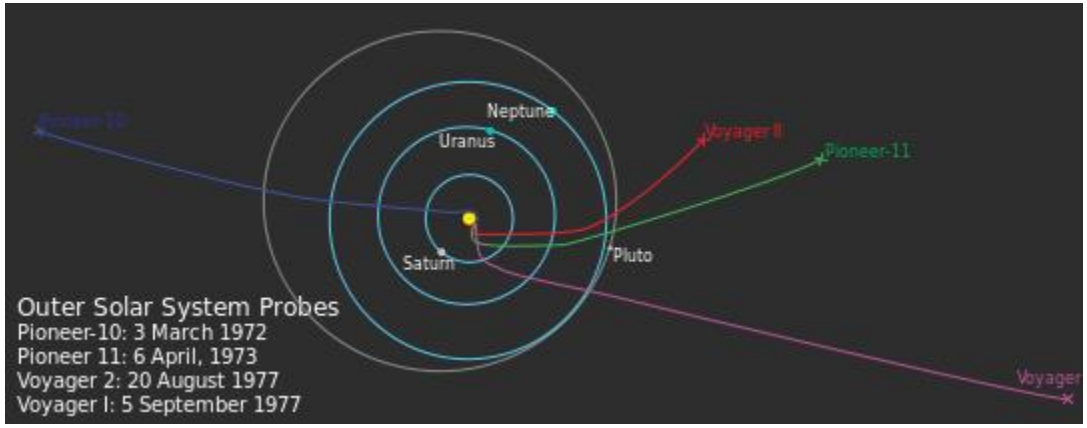
Сатурн и три от луните му: Тетис, Дион и Реа
(Вояджър 2, 04.08.1982)

Когато Вояджър 2 отива към Уран и Нептун, той започва да използва код на Рид-Соломон. Тези кодове не са бинарни, а са върху по-големи крайни полета, но са с по-високи коригиращи способности.



Изглед от вулканичните равнини на Тритон, спътник на Нептун, на базата на топографски снимки, направени от Вояджър 2, прелитайки покрай спътника през август 1989.

Двата Вояджъра вече са напуснали Слънчевата система. Заедно с Пионер 10 и 11 това са четирите междузвездни апарати.



Разстоянието на Вояджър 1 до Земята е 132 AE
(1 AE = 1 астрономическа единица е равна на средното разстояние от Земята до Слънцето ≈ 150 млн км) или 1.97×10^{10} km = 0.00209 светлинни години.
Сигналите от него достигат до нас за повече от 17 часа.

Интересно е да се отбележи, че на 22 април 2010 г. Вояджър 2 „се побърква” и дори се появяват информации, че е бил прехванат от НЛО. До въпросния 22 април сондата излъчва за едно денонощие доста скромния поток от информация от 160 бита в секунда, а след това започнала да подава много по-големи информационни масиви, състоящи се от неразбираема комбинация от знаци, букви и цифри.

Оказва се, че източник на проблемите е неизправност в една от клетките в паметта на бордовия компютър: стойността на клетката се е променила от нула в единица.
Инженерите са изпратили команда за рестартиране на машината и получените от Вояджър 2 сигнали са потвърдили, че рестартирането е било успешно.

Една от най-големите заслуги на Стефан Додунеков е създаването, започвайки от нулата, на българската школа в теорията на кодирането.
Неговите трудове покриват широк спектър от проблеми – от фундаментални задачи, със значение за абстрактната алгебра и крайните геометрии, до чисто приложни в областта на защитата на данни. Той се утвърждава като един от най-изтъкнатите учени по теория на кодирането в света.
Ще дадем идея за част от неговите най-добри постижения, които са доразвити от неговите ученици и са в област, в която българската школа е сред водещите в света.

Както отбелязахме, линейните кодове имат три основни параметъра, от които зависи тяхната скорост на предаване на информацията и коригиращата им способност:

(дължина n, размерност k, минимално разстояние d).

Най-добрите кодове измежду всички с фиксирани два от тези параметри са тези, за които третият параметър е оптимален.

Има редица връзки между тези параметри.

Граница на Сингълтън: $k \leq n - d + 1$.

(При фиксирани n и d третият параметър k не може да бъде много голям.) Кодът на Рид-Соломон, използван от Вояджър, е възможно най-добър, защото достига тази граница (k е максимално възможно).

Граница на Грисмер за бинарни кодове: $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$.

Граница на Плоткин: $d \leq nq^{k-1} \frac{q-1}{q^k-1}$.

Една от основните задачи на теорията на кодирането е намиране на кодове, които достигат известните граници, а когато такива кодове не съществуват, подобряване на съществуващите граници и намиране на кодовете с най-добри параметри.

Сред най-значимите приноси на Стефан Додунеков от края на 70-те и началото на 80-те години е решаването тези задачи за двоични кодове в размерност 7 и 8, резултат постигнат в ожесточена конкуренция с известни математици като Рей Хил, Хенк ван Тилборг, Тор Хелесет, Нобору Хамада и др.
През 90-те години заедно със свои ученици той въвежда и изследва т. нар. „кодове с максимално достижимо разстояние“ (почти-МДР кодовете). Тези работи събуждат огромен интерес в световен мащаб.
Съществен принос с фундаментален характер представляват изследванията на Стефан Додунеков върху самодуални кодове, както и върху сферични кодове и дизайни. Неговите изследвания от последните години по характеризацията на квазисъвършените кодове остават незавършени.