ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ ТЕКСТОВ С ОШИБКАМИ В СТЕГАНОГРАФИИ

А.К. Гуц, Т.В. Вахний
aguts@mail.ru, vahniytv@mail.ru
Омский государственный университет им. Ф. М. Достоевского

Предлагается использовать математические тексты для скрытой передачи битов информации в форме математических формул. Ошибка в формуле – это бит 0, формула без ошибки – 1. Весь текст, таким образом, несет скрытую последовательность битов: 011100101….

Любой математический текст может быть прочитан и понят только специалистов в конкретной области математики. Ошибки в формулах (в геометрических рисунках) в тексте, относящемся к элементарной математике, легко находятся выпускником средней школы, имевшим отличные оценки по математическим дисциплинам. Однако проверка текста по римановой геометрии требует уже отменных знаний в данной науке. И если знатока римановой геометрии можно еще найти в вузах областного центра, то проверка корректности текста в области алгебраической геометрии, или гомотопической топологии, или по теории топосов потребует, во-первых, осознания самого факта, что он относится к данным наукам, а, во-вторых, будет связана с весьма хлопотными поисками человека, способного его проверить, поскольку не в каждом регионе (стране!), такой нужный специалист найдется.

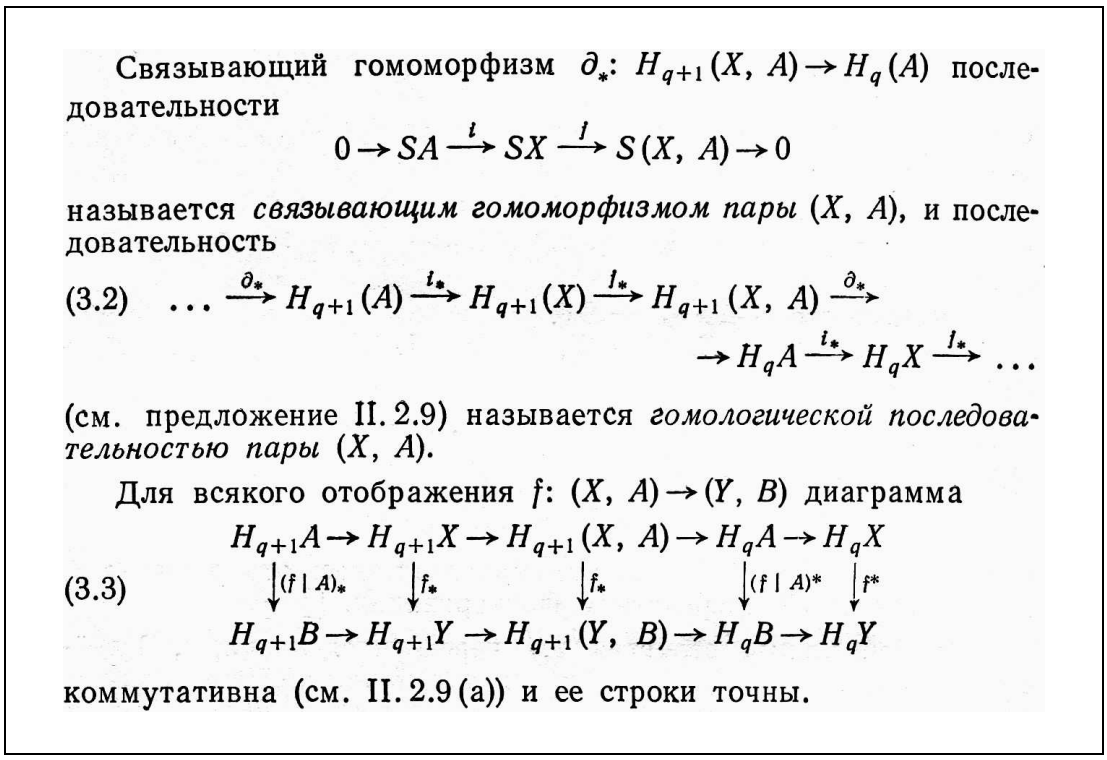
Ошибка может быть в формуле, в формулировке теоремы, в примере, в иллюстрации и т.д. Ключ при шифровании (дешифровании) − это, к примеру, договоренность допускать ошибки только в пронумерованных формулах. Очевидно, знание такого ключа резко сокращает время извлечения информации из полученного текста. Ошибка в пронумерованной формуле – это бит 0, следующая пронумерованная формула без ошибки – 1. Весь текст, таким образом, несет скрытую последовательность битов: 011100101…

На рис.1 приводится пример простейшего текста из теории гомологий (раздел алгебраической топологии). В него легко внести ошибки: достаточно повернуть в обратном направлении вертикальные стрелки в формуле (3.3), или вместо f_* написать f^*.

Этот пример показывает, что даже если воспользоваться возможностями современного Интернета и обратиться к специалисту-топологу в другой стране, то ему потребуется значительное время на проверку текста. Замечательная особенность приведенного примера, взятого из учебника А.Дольда «Лекции по алгебраической топологии» (1976), заключается в том,

что в формуле (3.3) имеются две опечатки: самые правые символы * должны стоять не как верхние индексы, а как нижние. Следовательно, нельзя доверить проверку правильности формулы (3.3) человеку, незнакомому с теорией гомологий.

Таким образом, поскольку в нумерованной формуле (3.3) имеются две ошибки, а формула (3.2) не содержит ошибок, то в свете данного тезиса можно заявить, что формулы (3.2), (3.3) несут три бита информации – 100, а учебник А.Дойча, безобидно стоящий на книжной полке, хранит в себе ключ для дешифровки некоторых криптографических сообщений.



Связывающий гомоморфизм ∂_*: $H_{q+1}(X, A) \to H_q(A)$ последовательности

$$0 \to SA \xrightarrow{i} SX \xrightarrow{j} S(X, A) \to 0$$

называется *связывающим гомоморфизмом пары* (X, A), и последовательность

(3.2) $$\ldots \xrightarrow{\partial_*} H_{q+1}(A) \xrightarrow{i_*} H_{q+1}(X) \xrightarrow{j_*} H_{q+1}(X, A) \xrightarrow{\partial_*} \to H_qA \xrightarrow{i_*} H_qX \xrightarrow{j_*} \ldots$$

(см. предложение II. 2.9) называется *гомологической последовательностью пары* (X, A).

Для всякого отображения f: $(X, A) \to (Y, B)$ диаграмма

(3.3)
$$\begin{array}{ccccccccc} H_{q+1}A & \to & H_{q+1}X & \to & H_{q+1}(X, A) & \to & H_qA & \to & H_qX \\ \downarrow{\scriptstyle (f \mid A)_*} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle (f \mid A)^*} & & \downarrow{\scriptstyle f^*} \\ H_{q+1}B & \to & H_{q+1}Y & \to & H_{q+1}(Y, B) & \to & H_qB & \to & H_qY \end{array}$$

коммутативна (см. II. 2.9 (а)) и ее строки точны.

Рис. 1. Пример текста из алгебраической топологии

В текстовой стеганографии существуют специальные программы, способные вносить скрытную информацию в текстовые файлы, например в виде определенного количества пробелов в конце каждой строки. Нетрудно создать программу, порождающую тексты по математике (физике, химии), способные тайно прятать информацию в форме ошибок в формулах.