

ინფორმაცია, ენტროპია და განუსაზღვრელობა  
შესავალი

1. ინფორმაციის ცნება. ინფორმაცია სხვადასხვა მოვლენებსა და ობიექტების შესახებ. ინფორმაციული გარემო, ინფორმაციის გაცვლისა და გადაცემის ზოგადი მიმოხილვა. ინფორმაციის დამუშავების პროცესები.

ინფორმაციის გადაცემის სქემატური წარმოდგენა კონკრეტულ მაგალითებზე დაყრდნობით. ინფორმაციული გარემოს განხილვა და გაანალიზება. ნებისმიერი დაუმუშავებელი ინფორმაციის დამუშავება.

ინფორმაცია ცხოვრების აუცილებელი ატრიბუტია. ადამიანი ცხოვრობს ინფორმაციულ გარემოში და გამუდმებით მონაწილეობს ინფორმაციულ პროცესებში.

ინფორმაციული ეწოდება ისეთ პროცესს, რომელიც დაკავშირებულია ინფორმაციის მიღებასთან, შენახვასთან, გარდაქმნა-ანალიზსა და გადაცემასთან. ასეთ პროცესს ინფორმაციის დამუშავების პროცესსაც უწოდებენ.

ინფორმაციის მოცულობისა და ინფორმაციული პროცესების ინტენსივობის ზრდამ ინფორმაციის ავტომატური დამუშავების აუცილებლობა წარმოშვა. ინფორმაციის დამუშავების უნივერსალურ ინსტრუმენტად კომპიუტერი იქცა.

ტერმინი „ინფორმაცია“ წარმოდგება ლათინური სიტყვიდან information, რაც ნიშნავს ცნობას, შეტყობინებას რაიმეს შესახებ. უფრო დაზუსტებით შეიძლება განვმარტოთ: ინფორმაცია არის შეტყობინებათა ერთობლიობა ობიექტების, მოვლენებისა და პროცესების შესახებ, რომელიც მიღების, შენახვის, გარდაქმნისა და გადაცემის ობიექტია.

ადამიანის ფსიქიკაზე დაკვირვებისას საქმე გვაქვს ინფორმაციის მიღებასა, დამუშავებასა, შენახვასა და გადაცემასთან. ინფორმაცია არის ცნობა სინამდვილის შესახებ, რომელიც მიიღება ან გადაიცემა სიგნალის საშუალებით. სიგნალი კი არის ფიზიკური ფაქტი, რომელსაც აღნიშნული ფუნქცია ახასიათებს (მაგ.: ასოები, ნახატი, სიტყვა, სინათლის ტალღები და სხვ.).

ინფორმაცია არ არის მატერიალური ან ენერგეტიკული ცნება. მისი არსება იმაშია, რომ მიმღებს უბიძგებს განსაზღვრული ქცევის არჩევაში – განსაკუთრებით აზროვნების სფეროში. ადამიანი ინფორმაციას ღებულობს სამი არხის საშუალებით:

ა. მემკვიდრეობითი ფაქტორებით (გენებით), რომლითაც ადამიანს მშობლებისაგან გადაეცემა ნივთიერი და სტრუქტურული ნიშნებით;

ბ. ადამიანებისაგან გადაეცემა ჩამოყალიბებული აზრებისა და მითითებების სახით (მაგ.: წიგნის საშუალებით);

გ. უშუალოდ გარემო სინამდვილისაგან.

ცხოველებისაგან განსხვავებით, რომლისთვისაც მემკვიდრეობითი ინფორმაცია განმსაზღვრელია, ადამიანისათვის მეტად დიდი მნიშვნელობა აქვს მეორე და მესამე არხით მიღებულ ინფორმაციებს. მათ ადამიანი ღებულობს სწავლისა და შრომის საშუალებით, ურომლისოდაც იგი ვერ ჩამოყალიბდება პიროვნებად.

აუცილებელ ინფორმაციათა მარაგით ადამიანის აღჭურვის თვალსაზრისით განსაკუთრებული მნიშვნელობა აქვს სკოლას, რომელიც მიზნობრივად ორგანიზებულ გარემოს წარმოადგენს. ყოველ სასწავლო საგანში მოსწავლე ითვისებს, ინახავს და შემდეგ თავის საქმიანობაში იყენებს განსაზღვრულ, ამ საგნისათვის დამახასიათებელ ინფორმაციებს.

ინფორმაცია სხვადასხვა მოვლენისა და ობიექტის შესახებ განსხვავებული შინაარსისაა. მეცნიერული მიდგომა ინფორმაციის ცნებისადმი მის შინაარსზე არ არის დამოკიდებული და საშუალებას გვაძლევს რაოდენობრივად შევაფასოთ იგი. ასეთი მიდგომა ინფორმაციას

განიხილავს, როგორც რაიმეს ცოდნის განუსაზღვრელობის საზომს ანუ არცოდნის შემცირების საზომს.

ვთქვათ, ვაგდებთ მონეტას სწორ ზედაპირზე. ამ დროს, ორი შესაძლო მოვლენიდან, ერთ–ერთი მონეტა დაეცემა პირით ან ზურგით. მონეტის აგდების წინ არსებობს განუსაზღვრელობა იმის შესახებ, თუ რომელი ზედაპირით დაეცემა მონეტა. მას შემდეგ, რაც მონეტა დაეცემა ანუ მოვლენა განხორციელდება, დგება სრული განსაზღვრულობა – მივიღებთ ინფორმაციას მისი შედეგის შესახებ. ამ შემთხვევაში შეიძლება ითქვას, რომ მიღებულმა ინფორმაციამ თავდაპირველი განუსაზღვრელობა ორჯერ შეამცირა, რადგან ორი შესაძლო შედეგიდან ერთი მივიღეთ. შეიძლება განვიხილოთ მოვლენები, რომელთაც ორზე მეტი შესაძლო შედეგი აქვს. მაგალიტად, კამათლის აგდების შემდეგ მივიღებთ შეტყობინებას ექვსი შესაძლო შედეგიდან ერთ–ერთზე. რაც მეტია მოვლენაში შესაძლო რაოდენობა, მით მეტია თავდაპირველი განუსაზღვრელობა და უფრო მეტი რაოდენობის ინფორმაციას შეიცავს შეტყობინება ასეთი მოვლენის შესახებ. ვინაიდან ინფორმაციას გააჩნია რაოდენობრივი მხარე, უნდა შეგვეძლოს მისი შეფასება ანუ გაზომვა.

### 1.1. ინფორმაციის გაზომვა, რაოდენობრივი ზომა

ინფორმაციის საზომი ერთეულია ბიტი. ეს არის ინფორმაციის რაოდენობა, რომელსაც შეიცავს შეტყობინება ორი შესაძლო შედეგის მქონე მოვლენის შესახებ. შეიძლება აგრეთვე ითქვას, რომ ბიტი ინფორმაციის ის რაოდენობაა, რომელიც მოვლენის შედეგის განუსაზღვრელობას ორჯერ ამცირებს.

მონეტის აგდების შედეგად მიღებული შეტყობინება შეიცავს სწორედ ერთ ბიტ ინფორმაციას, რადგან მისი შესაძლო შედეგების რაოდენობა ორის ტოლია.

იმისათვის, რომ შევაფასოთ ინფორმაციის რაოდენობა ორზე მეტი შესაძლო შემთხვევაში, საჭიროა მისი რაოდენობისა და შესაძლო შედეგების რიცხვის დაკავშირება. ეს კავშირი აისახება ფორმულით:  $N=2^I$ , სადაც  $I$  არის ინფორმაციის რაოდენობრივი ზომა, ხოლო  $N$  ყველა შესაძლო შემთხვევათა რაოდენობა ანუ სიმრავლე. აქედან გამომდინარე, აღნიშნული ფორმულიდან, ინფორმაციის რაოდენობრივი ზომა განისაზღვრება ლოგარითმით:  $I = \log_2 N$ . ორი შესაძლო შედეგის მქონე ( $N=2$ ) მოვლენის ინფორმაციის რაოდენობის შეფასებისას მივიღებთ:  $I = \log_2 N = \log_2 2 = 1$  ბიტი, რაც შეესაბამება საზომი ერთეულის ბიტის განმარტებას.

შეტყობინება ოთხი შესაძლო შედეგის მქონე მოვლენის შესახებ შეიცავს ორ ბიტ ინფორმაციას, რადგან  $\log_2 4 = 2$ . შეტყობინება კამათლის აგდების შედეგის შესახებ შეიცავს  $\log_2 6$  ბიტ ინფორმაციას და ა.შ.

ერთი შესაძლო შედეგის მქონე მოვლენისათვის  $I = \log_2 1 = 0$ , ე.ი. შეტყობინება ამგვარის მოვლენის შესახებ საერთოდ არ შეიცავს ინფორმაციას, რადგან მისი შედეგი წინასწარაა განსაზღვრული.

ინფორმაციის ლოგარითმული ზომა უნივერსალური საზომია, რადგან ითვალისწინებს მხოლოდ მოვლენის შესაძლო შედეგების რაოდენობას და მის შინაარსზე არ არის დამოკიდებული.

„ინფორმაციის“ ცნება ერთ–ერთი ძირითადია ინფორმაციული სისტემების განხილვისას. არსებობს ინფორმაციის მრავალი განსხვავებული თვალსაზრისი და განსაზღვრებები ზოგადი ფილოსოფიურიდან (როგორც რეალური სამყაროს ასახვა–გამოხატულება) ყველაზე კერძო პრაქტიკულ განსაზღვრებამდე (როგორც–ცნობები, რაც გამოიხსნება ინფორმაციის დამუშავების, შენახვისა და გადაცემისათვის). მნიშვნელოვანია ნ.ვინერის აზრი, რომ „ინფორმაცია არის ინფორმაცია და არა მატერია ან ენერგია“ [ვინ]. ამ საკითხების განხილვა–წარმოჩენა სცილდება სასწავლო საგნის მიზნებს და ამიტომ ქვემოთ განხილულია საკითხები ინფორმაციის რაოდენობრივი განსაზღვრებისა (კლასიკური გაგებით), რაც კოდირების ოპტიმალობასა და გადაცემის საიმედოობასთან არის დაკავშირებული.

ინფორმაციის გამოხატვის საშუალებები მატერიალურ-ენერგეტიკულია და ჩვენს შემთხვევაში წარმოადგენს ფიზიკურ სიგნალებს, ასო-ნიშნებს, ციფრულ ჩანაწერებს, ფიგურებსა და სხვ. საუბარი ინფორმაციის დაცვის სისტემის შესახებ ფორმალურია, თუ ის ინფორმაციის არსებობის თვით ფაქტს არ ითვალისწინებს. ნებისმიერი კოდი, ინფორმაციის მატარებელია. კოდირების სისტემები ინფორმაციის დამუშავების, გადაცემისა და დამახსოვრებისათვის იქმნება, მაგრამ ამით ლოგიკური (გენეტიკური) და სხვა კოდებისაგან განსხვავებით ინფორმაციის დაცვისათვის გამოიყენებული კოდების მთავარი ფუნქცია მიმდინარე პროცესების დაცვაა გარეშე ზემოქმედებისაგან. მიუხედავად ამისა არ უნდა დაგვავიწყდეს, რომ ინფორმაციის გადაცემისას ბუნებასა თუ ცოცხალ გარემოში, ტექნიკურ სისტემებსა თუ საზოგადოებაში, როგორც არ უნდა იყოს მისი წყარო თუ მომხმარებელი, იქმნება ინფორმაციული გარემო, რომელშიც კოდირების სისტემები საერთო ინფორმაციულ პროცესს ექვემდებარებიან, ხოლო ინფორმაციული სინერგულობა (ურთიერთშეთანხმებულობა, ურთიერთთანწყობა) თვისობრივად მსგავს და პროცესებისათვის საერთო სტრუქტურათა წარმოქმნას განაპირობებს, რაც განსაკუთრებით კოდირების სისტემებით აისახება და ვლინდება.

## **1.2. ინფორმაცია და მისი რაოდენობის განსაზღვრება. ინფორმაციის ოპტიმალური კოდირება და გადაცემის საიმედოობა**

გარე სამყაროს მთლიანობის ერთ-ერთი ნიშანდობლივი თვისება მისი ინფორმაციული მთლიანობაა.

ინფორმაციის გადაცემისას (ბუნებასა, ტექნიკურ სისტემებსა თუ საზოგადოებაში) იქმნება ინფორმაციული გარემო, რომელშიც კოდირების სისტემები საერთო ინფორმაციულ პროცესს ექვემდებარებიან, ხოლო ინფორმაციული სინერგულობა (ურთიერთშეთანხმებულობა, ურთიერთთანწყობა) თვისობრივად მსგავს და საერთო სტრუქტურათა წარმოქმნას განაპირობებს, რაც განსაკუთრებით კოდირების სისტემებით აისახება და ვლინდება.

აქედან გამომდინარე, ნებისმიერი კოდი მოიცავს გარკვეულ ინფორმაციას. ზოგი მათგანი სტრუქტურული და ფუნქციონალური თვისებისაა (მაგალითად, გენეტიკური), ზოგი კი გამიზნულია მხოლოდ ინფორმაციის დამუშავებისა და გადაცემისათვის და სხვა, თუმცა მკვეთრი საზღვრის გავლება მათ შორის ხშირად შეუძლებელია.

კოდირების წინამდებარე საგანი ინფორმაციის დაცვისადმი განკუთვნილი, ამიგომ ბუნებრივი და მიზანშეწონილია გარკვეული ფორმით თუ ოდენობით განხილული იყოს ინფორმაციის თეორიის ძირითადი საფუძვლები და შედეგები.

არსებობს "ინფორმაციის" მრავალი განსხვავებული განსაზღვრება ზოგად ფილოსოფიურად (როგორც-რეალური სამყაროს ასახვა-გამოხატულება) ყველაზე კერძო პრაქტიკულ განსაზღვრებამდე (როგორც – მონაცემები, გამიზნული მათი დამუშავების, გადაცემისა და დამახსოვრებისათვის). აღსანიშნავია გერმინ "ინფორმაციის" მრავალმხრივი (უშუალო, მაგრამ ხშირად გაუცნობიერებელი) გამოყენება ყოველდღიურ ცხოვრებაში: "ინფორმაციული საშუალებები", "მიღებული ინფორმაცია", "არასრული ინფორმაცია", "ინფორმაციული ომი", "ინფორმაციული გარემო" და ა.შ., რაც წარმოადგენს გერმინ "ინფორმაციასთან" დაკავშირებულ ცნებათა არასრულ ჩამონათვალს. მნიშვნელოვანია ნორბერტ ვინერის აზრი, რომ "ინფორმაცია არის ინფორმაცია და არა მაგერია ან ენერგია". ამ საკითხების განხილვა სცილდება სასწავლო საგნის მიზნებს, ამიგომ პირველ თავში განხილულია მხოლოდ საკითხები ინფორმაციის რაოდენობის განსაზღვრებისა (მისი კლასიკური გაგებით), ასევე, – საკითხები ინფორმაციის კოდირების ოპტიმალულობისა და გადაცემის საიმედოობის შესახებ).

## **1.3. ენტროპია და ინფორმაცია. ენტროპია, როგორც განუსაზღვრელობის ხარისხი**

ინფორმაციის წარმოქმნის პროცესი დაკავშირებულია რაიმე საგნის (ობიექტის) ან საზოგადოდ სისტემის სინთეზსა და ცვალებადობასთან. შესაძლოა იცვლებოდეს საგნის მდებარეობა ან ფორმა, ადგილი ჰქონდეს ვნობილ ბუნებრივ მოვლენებს (მოღრუბლულობა, წვიმა, ქარი და სხვ.), ყოველივე მას, რაც მოსალოდნელია, მაგრამ დანამდვილებით მათი მოხდენის წინასწარი

ხედვა შეუძლებელია, რადგან დაკავშირებულია გარკვეულ შემთხვევით მოვლენებსა და ხდომილობებთან. ესაა ნებისმიერი სფერო იქნება ის ინფორმაციული საშუალებები, გასართობი თამაშობანი, თუ ჩვეულებრივი საყოფაცხოვრებო გარემოებები.

შესაძლოა, ჩვენ თავად ვატარებდეთ ცდას, დაკავშირებულს შემთხვევით ხდომილობებთან (სიდიდეებთან). ყოველ ასეთ შემთხვევაში ვარაუდი ამა თუ იმ ხდომილობის მოხდენისა ეყრდნობა ხდომილობათა ალბათობებს. ის რომ, მაგალითად, კამათელის გაგორების შემთხვევაში რომელიმე კონკრეტული  $x_i$ -რი, სადაც  $i = 1, 2, \dots, 6$ , რიცხვის მოსვლის ალბათობა ცნობილია (და ამ შემთხვევაში  $p(x_i) = 1/6$ -ს), გვაძლევს შესაძლებლობას შევიქმნათ მოცემული ხდომილობის მოხდენის შესახებ. ე.ი. ხდომილობის ალბათობა განსაზღვრავს ჩვენი ვარაუდის ხარისხს სათანადო ხდომილობის შესახებ. შეიძლება დაისვას კითხვა, – როგორია კავშირი ხდომილობის ალბათობასა (ანუ ვარაუდსა) და მიღებულ ინფორმაციას შორის (ხდომილობის მოხდენის შემთხვევაში)? პასუხი კითხვაზე.

განვიხილოთ განსხვავებული შემთხვევა. ის ფაქტი, რომ ხვალ დედამიწა არ შეწყვეტს ბრუნვას თავისი ღერძის გარშემო, დღეისათვის ყველასათვის ცნობილია და ამიტომ ხვალინდელი დღე – დედამიწის შემობრუნება  $360^\circ$ -ით სრულიად მოსალოდნელია და ამ გაგებით შეიძლება ასევე ითქვას, რომ ახალ ინფორმაციასაც არ შეიცავს (თუმცა არსებობს საჩინააღმდეგოს გარკვეული ალბათობა, რაც ყოველდღიურობაში, მისი სიმცირისა გამო, ჩვეულებრივ უგულებელყოფილია).

#### 1.4.ენტროპია და ინფორმაცია. ენტროპია, როგორც განუსაზღვრელობის ხარისხი

შევთანხმდეთ, რომ ინფორმაციის წარმოქმნის პროცესი დაკავშირებულია გარკვეული საგნის (სისტემის, ანუ, საზოგადოდ, – ობიექტის) სინთეზსა და ცვალებადობასთან. შესაძლოა იცვლებოდეს ობიექტის მდებარეობა ან ფორმა, ადგილი ჰქონდეს ბუნებრივ მოვლენებს (ვთქვათ, უღრუბლო ცაზე ღრუბლების გამოჩენა, წვიმის ან ქარის ინტენსიურობის ცვლილება, კამათლის გაგორების შემთხვევაში გარკვეული რიცხვის მოსვლა. ჩვენთვის, ცხადია, საინტერესო მაგალითს წარმოადგენს ინფორმაციის წყაროს გამოსავალზე გარკვეული სიგნალის გამოჩენა და სხ.). ყველა ამ შემთხვევაში ვგულისხმობთ, რომ მოსალოდნელი ცვლილება შეიძლება დასრულდეს ორი ან მეტი შედეგიდან ერთ-ერთით (თუ მდგომარეობის უცვლელად შენარჩუნებასაც ერთ-ერთ შესაძლო შედეგად მივიღებთ), რომლის წინასწარ გამოცნობა შეუძლებელია; შეუძლებელია, თუ საქმე გვაქვს შემთხვევით მოვლენებსა და ხდომილობებთან ისე, როგორც მათ ალბათობის თეორია განიხილავს.

მაშასადამე, საკითხის ასე დასმის დროს არ გვაინტერესებს, თუ რა ინფორმაციას მოიცავს ობიექტი მასზე დაკვირვებამდე. გვაინტერესებს, თუ რა რაოდენობის ინფორმაციას შეიძენს დამკვირვებელი დაკვირვების (ანუ ობიექტის ცვლილების) შედეგად, ე.ი. ინფორმაცია, განსახილველი მიდგომის პირობებით, მიიღება შემთხვევით ხდომილობებზე დაკვირვების დროს.

დავუშვათ, რომ ვატარებთ ცდას, რომლის შედეგი შემთხვევითი ხდომილობებია. დამკვირვებლის ვარაუდი ხდომილობის მოხდენის (ანუ ცდის შედეგის) შესახებ ეყრდნობა ხდომილობათა ალბათობებს. მაგალითად, კამათლის გაგორებისას რომელიმე  $x_i$ -ური ( $i=1, \dots, 6$ ) რიცხვის გაჩენის ალბათობა ცნობილია და  $P(x)=1/6$ -ს. შესაბამისად, – ხდომილობების ალბათობები განსაზღვრავს ცდის შედეგის გაურკვევლობას (მის განუსაზღვრელობას), რასაც ჩვენი ვარაუდი ემყარება. შეიძლება დაისვას კითხვა – რა რაოდენობის ინფორმაციას ღებულობს დამკვირვებელი, როგორც ინფორმაციის მომხმარებელი, ცდის ერთ-ერთი შედეგის შემთხვევაში, ანუ რა რაოდენობის ინფორმაცია მიიღო მომხმარებელმა, როდესაც შემთხვევითი ცვლილება გარკვეული შედეგით დასრულდა? რადგან ცდის განუსაზღვრელობა დამოკიდებულია ხდომილობის ალბათობებზე, მაშასადამე ცდის შედეგად მიღებული ინფორმაცია დამოკიდებულია ხდომილობის ალბათობებზე და ინფორმაციის რაოდენობა არის ხდომილობების ალბათობათა ფუნქცია).

განვიხილოთ განსხვავებული მაგალითი. დედამიწა რომ არ შეწყვეტს ბრუნვას თავისი ღერძის გარშემო, დღეს საზოგადოდ ცნობილია და ხვალინდელი დღე – დედამიწის

შემობრუნება 360<sup>0</sup>-ით – სრულიად მოსალოდნელია და, ამიგომ, ახალ ინფორმაციას არ შეიცავს (თუმცა თეორიულად არსებობს საწინააღმდეგო შედეგის ალბათობა, რაც მისი სიმცირის გამო ჩვეულებრივ უგულებელყოფილია). როგორც ვხედავთ, თუ შესაძლო ცვლილების ალბათობა ერთის ტოლია, მაშინ შედეგს ახალი ინფორმაცია არ გააჩნია.

მაშასადამე, ინფორმაციას არ წარმოქმნის ხდომილობა ერთის ტოლი ალბათობით – აუცილებელი ხდომილობა (ანუ ობიექტი, რომლის ცვლილების შედეგი წინასწარ ცნობილია) და, ცხადია, არც ხდომილობა, რომლის ალბათობა ნოლის ტოლია – შეუძლებელი ხდომილობა (ანუ ობიექტი, რომელიც არ იცვლება).

გემოაღნიშნულის თანახმად, დამკვირვებელმა ინფორმაცია შეიძლება მიიღოს მხოლოდ ცვალებად გარემოზე დაკვირვების შედეგად და არა გარემოში, რომელიც ცვლილებას არ განიცდის ან ცვლილებები დეტერმინირებული ხასიათისაა (დეტერმინირებულია ცვალებადობები, როდესაც ობიექტის ერთი მდგომარეობიდან მეორეში გადასვლა წინასწარ ცნობილ კანონს ემორჩილება).

აღსანიშნავია, რომ ინფორმაციის წარმოქმნა დამოკიდებულია როგორც დასაკვირვებელ მოვლენაზე, აგრეთვე თვით დამკვირვებელზეც. შესაძლოა, ერთი დამკვირვებლისათვის ცვალებადობები შემთხვევითი ხასიათისაა და ინფორმაციული, მაგრამ მეორესთვის – დეტერმინირებული და, მაშასადამე, არაინფორმაციული.

ამრიგად, ინფორმაციის რაოდენობის განსაზღვრის საფუძველი არის ობიექტის შესაძლო ცვლილებათა შედეგის განუსაზღვრელობა, ანუ – არასრული ინფორმაციულობა. ცხადია, ვინც ყველაფერი იცის, ახალ ინფორმაციას ვერ შეიძენს, ე.ი. ინფორმაციის რაოდენობასა და განუსაზღვრელობის რაოდენობას (განუსაზღვრელობის ხარისხს) შორის შეიძლება გოლობის ნიშანი დაისვას).

რა თვისებებს უნდა აკმაყოფილებდეს განუსაზღვრელობის ფუნქცია? გემოთ ავლენიშნეთ, რომ განუსაზღვრელობა და ინფორმაციის რაოდენობა დამოკიდებულია ხდომილობათა ალბათობებზე. რაც უფრო მცირეა ხდომილობის ალბათობა, მით მეტია მისი მოხდენის შემთხვევაში მიღებული ინფორმაცია: გაფხულის დღეებში თოვლის მოსვლას დიდი რაოდენობის ინფორმაცია გააჩნია. ხდომილობის ალბათობის მაღალი მნიშვნელობის დროს შესაბამისი შედეგი ნაკლებად ინფორმაციულია: გამთრის დღეებში თოვლის მოსვლას ნაკლები ინფორმაცია გააჩნია.

როდესაც მეგობრისაგან ბარათს ხშირად ვღებულობთ, მაშინ მორიგი ბარათის მიღებას (კერძოდ, თვით ფაქტს ბარათის მიღებისას და არა მის შინაარსს, – ამ საკითხს ქვემოთ 1.2 განაკვეთში დავუბრუნდებით) არ ახლავს დიდი რაოდენობის ინფორმაცია განსხვავებით იმ შემთხვევისაგან, როდესაც ბარათის ავტორისაგან დროის ხანგრძლივ პერიოდში არავითარი ინფორმაცია არ არსებობდა. ბარათის მიღება ამ შემთხვევაში ნაკლებად მოსალოდნელია და შედარებით დიდი რაოდენობის ინფორმაციას შეიცავს.

გემოთ განხილულ მაგალითებში ძირითადი ყურადღება ექცევა ხდომილობათა ცალკეულ ალბათობებს, რაც არის საკითხის ერთი მხარე (აქ, კერძოდ, გასათვალისწინებელია შემდეგი გარემოება – რადგან პროცესი შემთხვევითი ხასიათისაა, საჭიროა განისაზღვროს განუსაზღვრელობისა და შესაბამისი ინფორმაციის საშუალო მნიშვნელობა). მართლაც, თუ მხოლოდ ხდომილობათა ცალკეულ ალბათობებს მივიღებთ მხდეველობაში და დავუშვებთ, რომ  $x_i$ -ური ხდომილობის ალბათობა  $P(x_i) \neq 0$ , მაშინ მიღებული ინფორმაცია შეიძლება წარმოვიდგინოთ როგორც  $P(x_i)$  ალბათობის  $I(x_i) = f(P(x_i))$  ფუნქცია და შემდეგი სახით ჩავწეროთ:

$$I(x_i) = 1/P(x_i) \quad (1.1.1)$$

(1.1.1) ფუნქციის მიმართ საყურადღებოა შემდეგი არსებითი შენიშვნა. განუსაზღვრელობის ფუნქცია დამოკიდებული უნდა იყოს არა ცალკეულ შედეგთა ალბათობაზე, არამედ ხდომილობათა სრული სისტემის ალბათობებზე, რაც სისტემის ენტროპიის ზომის განსაზღვრისათვის არის აუცილებელი. ქვემოთ ცხადი გახდება, რომ (1.1.1) დამოკიდებულება არასრული და წინააღმდეგობრივია, თუმცა მასში რაციონალურია განუსაზღვრელობისა და ხდომილობის ალბათობის ურთიერთდაკავშირებულობა

(იგულისხმება, რომ ხდომილობები ადგენენ ხდომილობათა სრულ ჯგუფს და შესრულებულია ნორმირების აქსიომა.)  
აღნიშნული საკითხის განხილვამდე განვიხილოთ რაოდენობრივ და სემანტიკურ ინფორმაციათა არსებითი განსხვავებულობა.

## 1.5. რაოდენობრივი და სემანტიკური ინფორმაცია

წინამდებარე საგნის თემატიკა არ ითვალისწინებს ინფორმაციის სემანტიკური (შინაარსობრივი) მნიშვნელობის განხილვას. სემანტიკური ინფორმაციის საკითხი რთული და პრობლემატურია და არ არის სრულად დამუშავებული (სემანტიკური ინფორმაციის რაოდენობის, როგორც სელექტიური ინფორმაციის განსაზღვრა და მისი სპეციალურ ფუნქციათა სახით წარმოდგენა კერძო შემთხვევებში სავსებით რეალურია.) მაგრამ რაოდენობრივ და სემანტიკურ ინფორმაციათა შორის განსხვავების აღნიშვნა და მისი გარკვევა საკუთრივ რაოდენობრივი ინფორმაციის ფორმულირების გაცნობიერებისათვის არის აუცილებელი.

განსხვავება ითქმის ყოველთვისაა. მას ძირითადად დამკვირვებელი, ანუ მომხმარებელი, განაპირობებს, რაც ჩანს ზემოთმოყვანილი მაგალითებიდანაც. კამათელზე რომელიმე რიცხვის, ვთქვათ, 6-ის გამოჩენა დამკვირვებლისათვის ერთ შემთხვევაში მეტად მნიშვნელოვანი, საყურადღებო და ინფორმაციულია მაშინ, როდესაც სხვა შემთხვევაში – ნაკლებად მნიშვნელოვანი. იგივე ითქმის მეგობრისაგან მიღებული ბარათის შემთხვევაში: ერთ ბარათს მიმღებისათვის (როგორც ადრესატისათვის), შესაძლოა, განსაკუთრებული მნიშვნელობა ჰქონდეს, სხვა კი იყოს ნაკლებად საგულისხმო და შინაარსიანი, მიუხედავად იმისა, თუ რამდენად ხშირად ღებულობს ბარათს ადრესატი. განსაკუთრებული მნიშვნელობა აქვს მომხმარებლის განწყობასაც განურჩევლად იმისა, თუ რას აღიქვამს; შედეგი შესაძლოა სრულიად განსხვავებული იყოს.

ერთი მკითხველისათვის ან მსმენელისათვის რაიმე წიგნი თუ მუსიკალური ნაწარმოები შინაარსიანი და ემოციური შეიძლება იყოს, მეორესთვის კი – არა. ამიტომ ნებისმიერი მოვლენის თუ ხდომილობის სემანტიკური ინფორმაციის მნიშვნელობა და მისი “ტევადობა” მრავალ ფაქტორზე და განსხვავებულ მომხმარებელზე დამოკიდებული სიდიდეა (სუბსტანტია) და ამდენად ცალსახა ზოგად ობიექტურ გაზომვას არ ექვემდებარება.

ვთქვათ, ერთიდაიგივე კოლოფის, ყუთის, თუ ჩანთის მოცულობის რაოდენობრივი (განზომილებითი) სიდიდის დადგენა შეიძლება, მაგრამ მასში არსებული საგნების სემანტიკური მნიშვნელობის დასადგენად ობიექტური შეფასების მიღება სხვადასხვა მომხმარებლის შემთხვევაში, საზოგადოდ, შეუძლებელია.

ერთი სიტყვით, ერთიდაიმავე მოვლენაში, თუ კოდურ გამოსახულებაში, სხვადასხვა დამკვირვებელმა შეიძლება დაინახოს არა მხოლოდ სხვადასხვა აქტუალობის შემცველი ინფორმაცია, არამედ ინფორმაცია, განსხვავებული თავისი შინაარსითაც, რაც მოვლენის განსხვავებულ შეფასებას (აღქმას) განაპირობებს.

შემდგომში ინფორმაციის განსაზღვრისას განვიხილება ინფორმაციის რაოდენობრივი, არასემანტიკური, ასპექტი, რაც დაკავშირებულია ხდომილობათა სრულ სისტემასთან განურჩევლად იმისა, თუ რა შინაარსისა და დანიშნულების ინფორმაციულ პროცესს წარმოადგენს მოცემული სისტემა.

## 1.6. ენტროპიისა და ინფორმაციის რაოდენობის ზომა

ინფორმაციის რაოდენობის ზომა დაკავშირებულია ობიექტის ენტროპიის (განუხაზღვრელობის) ზომასთან, რაც (როგორც ზემოთ იყო აღნიშნული) ეფუძნება ხდომილობათა სრული სისტემის ალბათობებს.

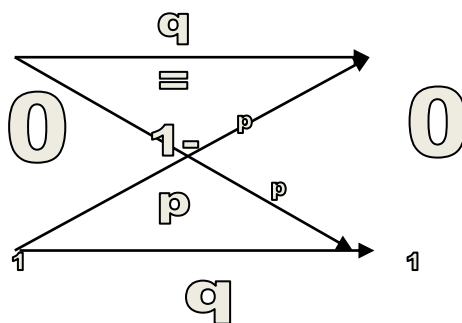
საკუთრივ ინფორმაციის განსაზღვრამდე განვიხილოთ ინფორმაციის გადაცემის პრინციპული სქემა კავშირის დისკრეტული ორობითი სიმეტრიული არხის მეშვეობით (რათა ყურადღება

გამახვილდეს ინფორმაციის გადაცემის პროცესის ფიზიკურ მხარეზე). დავუშვათ, რომ დროის გარკვეულ  $t$  მონაკვეთში გადაიცემა ცალკეული  $i$ -ური სიმბოლო. დროის შედარებით გრძელ  $T$  მონაკვეთში შეიძლება გადაიცეს  $n=T/t$  სიმბოლო, ანუ  $n$  - თანმიმდევრობა სიმბოლოებისა:

$$v = (v_1, \dots, v_n) \in V_n, \quad (1.3.1)$$

სადაც  $V_n$  ვექტორული სივრცეა  $GF(2)$  ველზე (სიმარტივისათვის განიხილება კოდირების ორობითი სისტემა. ზოგადად კოდირების სისტემას განიხილავენ  $GF(q)$  ველზე. (იხ.მე-2 თავი)).

ფიზიკურად კავშირის არხში გადაიცემა გარკვეული სიმბლავრისა და ენერგიის იმპულსები. იმპულსის გადაცემას დროის  $t$  მონაკვეთში პირობითად შეესაბამება  $v_i=1$ , ხოლო პაუზას –  $v_i=0$  სიმბოლო. დავუშვათ, რომ კავშირის არხში სიმბოლოს უშეცდომოდ გადაცემის ალბათობა არის  $q$ , შეცდომის ალბათობა –  $p=1-q$ ;  $p$  არის ალბათობა იმისა, რომ 1-ის გადაცემის შემთხვევაში არხის მეორე მხარეს მივიღებთ 0-ს ან 0-ის გადაცემისას – 1-ს. განიხილება დისკრეტული ორობითი სიმეტრიული არხი დამოუკიდებელი შეცდომებით, ანუ არხი მეხსიერების გარეშე, რომლის პრინციპული სქემა მოცემულია სურ.1.1-ზე:



სურ.1.1.

დავუბრუნდეთ სისტემის განუსაზღვრელ  $1$  ის საკითხს.

=

p

2 კრიპტოგრაფია. მართვის პროცესის ინფორმაციული მოდელი. ინფორმაციის გადაცემის მახასიათებლები. ინფორმაციის წყარო, ინფორმაციის მიმღები და საინფორმაციო არხი, მისი გამტარუნარიანობა. მონაცემთა ტიპები და სტრუქტურები.

კრიპტოგრაფია. ინფორმაციის დაცვის მეთოდები. ინფორმაციის გარემოს საიმედოობის განსაზღვრა, მისი დამოკიდებულება სხვა პარამეტრებზე. კავშირის არხის ტიპების განხილვა.

კრიპტოგრაფია. მართვის პროცესის ინფორმაციული მოდელი. ინფორმაციის გადაცემის მახასიათებლები. ინფორმაციის წყარო, ინფორმაციის მიმღები და საინფორმაციო არხი, მისი გამტარუნარიანობა. მონაცემთა ტიპები და სტრუქტურები.

3. დასამუშავებელი ინფორმაცია, ინფორმაციის დამუშავების პროცესი. ინფორმაციის კოდირება და დეკოდირება ორობით და ათობით ფორმებში.

დასამუშავებელი ინფორმაცია, ინფორმაციის დამუშავების პროცესი. ინფორმაციის კოდირება და დეკოდირება ორობით და ათობით ფორმებში, კონკრეტული მაგალითები.

4. ინფორმაციის ტიპები. რიცხვითი, ტექსტური, გრაფიკული, დიაგრამული, ლოგიკური. ინფორმაციის გადაცემისა და მიღების სქემატური წარმოდგენა და გარჩევა.

ინფორმაციის გადაცემისა და მიღების სქემატური წარმოდგენა. სხვადასხვა სახის ინფორმაციის კოდირებისა და დეკოდირების პროცესების განხილვა, მაგალითები.

5. ინფორმაციის იერარქიული სტრუქტურა. ინფორმაციის ქსელური სტრუქტურა. ინფორმაციის ცხრილური სტრუქტურა. ინფორმაციის სქემატური წარმოდგენა სტრუქტურის სხვადასხვა სახეობების მიხედვით.

ინფორმაციის იერარქიული, ქსელური და ცხრილური სტრუქტურები. ინფორმაციის წარმოდგენა ხისებრი სახით, მაგალითები.

6. ალგორითმიზაცია. ამოცანათა დასმა, ფორმალიზაცია, ალგორითმის დამუშავების ეტაპები. სქემატური მოდელის შედგენა.

კონკრეტული ამოცანების დასმა და მისი ალგორითმიზაცია. ალგორითმის დამუშავება, მაგალითები.

7. ინფორმაციის რაოდენობრივი და სემანტიკური ზომები, მათი გამოთვლის გზები. ინფორმაციის წარმოდგენის ფორმები. ინფორმაციული გარემო. უცვლელი და დეტერმინირებული გარემო. ინფორმაციის მიღების გზები. ინფორმაციის რაოდენობრივი ზომის დამოკიდებულება მის ყველა შესაძლო შემთხვევათა რაოდენობაზე, ანუ სიმრავლეზე.

ინფორმაციის რაოდენობრივი და სემანტიკური ზომები, მათი გამოთვლა. ინფორმაციის სიმრავლის, ჩასატარებელი ოპერაციებისა და ალბათობების დადგენა, კონკრეტული მაგალითებისათვის.

8. ხდომილობათა ალბათობები. შეცდომისა და სწორად მიღების ალბათობები. არხის განუსაზღვრელობა ანუ ენტროპია. ინფორმაციის გადაცემის სქემატური წარმოდგენა. ხმაურიანი და უხმაურო არხები.

ხდომილობათა ალბათობების განსაზღვრა. განუსაზღვრელობისა და ენტროპიის გამოთვლა უხმაურო და ხმაურიანი არხების დროს.



9. ინფორმაციის გადაცემის საიდუმლო არხები, ანუ სიმეტრიული სისტემები. ინფორმაციის დაშიფვრა-გაშიფვრა. ცეზარის, ვიჟინერის და ვერნამის მეთოდები. მეთოდთა მახასიათებლები და მათი შედარებები. გალუას ველები. წრფივი კოდების საზღვრები. სიმეტრიული სისტემები. ცეზარის, ვიჟინერის და ვერნამის მეთოდებზე დაყრდნობით კონკრეტული ამოცანების დასმა, ამოხსნა და მახასიათებლების გამოთვლა.

10. შებრუნებული მატრიცის მეთოდი. მისი გამოყენება ინფორმაციის დაცვისათვის. მისი მახასიათებლები და შედარება აღნიშნული მეთოდის მახასიათებლების სხვა არსებული მეთოდების მახასიათებლებთან. სიმეტრიული სისტემის მეთოდთა კრიპტოსირთულე. შებრუნებული მატრიცის მეთოდის მიხედვით ინფორმაციის დაშიფვრისა და გაშიფვრის მაგალითები. მისი მახასიათებლების გამოთვლა, როგორცაა: სისწრაფე, სიმრავლე, ჩასატარებელი ოპერაციების რაოდენობა და ალბათობა.

11. ინფორმაციის გადაცემის ღია არხის ანუ ასიმეტრიული სისტემის მეთოდები. დიფი-ჰელმან-მერკლეს მეთოდი. მისი გაანალიზება და გამოყენების შესაძლებლობები. მახასიათებლები - სიჩქარე, დრო, ალბათობა, ჩასატარებელი ოპერაციების რაოდენობა, საიმედოობა.

ასიმეტრიული სისტემები. დიფი-ჰელმან-მერკლეს მეთოდზე დაყრდნობით ინფორმაციის დაცვის განხორციელება. გასაღების გამოთვლა. ინფორმაციის დაშიფვრა-დეშიფრაციის პროცესის განხილვა-გაანალიზება.

12. ასიმეტრიული სისტემის რაივესტ-შამირ-ეიდელმანის ალგორითმი. მახასიათებლების გამოთვლა. მახასიათებლების მიხედვით მისი შედარება დიფი-ჰელმან-მერკლეს მეთოდის მახასიათებლებთან. მათი ანალიზი.

ასიმეტრიული სისტემის რაივესტ-შამირ-ეიდელმანის ალგორითმის მიხედვით ინფორმაციის დაცვა, დასაიდუმლოება. კონკრეტული მაგალითების განხილვა, გაანალიზება და მისი შედარება დიფი-ჰელმან-მერკლეს მეთოდთან.

13. ასიმეტრიული სისტემის ელ-გამალის ალგორითმი. ინფორმაციის გადაცემის პროცესი. მახასიათებლების გამოთვლა და შედარება სხვა ღია არხის მეთოდებთან. მისი გამოყენების არეალი. ღია არხის მეთოდთა კრიპტოსირთულის დადგენა.

ასიმეტრიული სისტემის ელ-გამალის ალგორითმის განხილვა. დაშიფრული ინფორმაციის გადაცემა და შემდგომ გაშიფვრის პროცესი, კონკრეტული მაგალითები. მახასიათებლების გამოთვლა და მისი შედარება სხვა მეთოდებთან.

14. ენტროპიისა და ინფორმაციის რაოდენობრივი ზომა. კოდირების ორობითი და ათობითი სისტემები. ინფორმაციის გადაცემა კავშირის არხში. შენონის ორი ძირითადი თეორემა უხმაურო და ხმაურიანი არხებისათვის. ინფორმაციის სტაციონალური და ერგოდული წყაროები.

ენტროპიისა და ინფორმაციის რაოდენობრივი ზომების განსაზღვრა. შენონის ორი ძირითადი თეორემა უხმაურო და ხმაურიანი არხებისათვის, მაგალითები.

15. ინფორმაციის გადაცემის სისწრაფე და არხის გამტარუნარიანობა. მათი განსაზღვრა და გამოთვლა. ინფორმაციის წყაროს ენტროპია.  
ინფორმაციის გადაცემის სისწრაფისა და არხის გამტარუნარიანობის გამოთვლის მექანიზმი.