ČASTI MODELU INFORMAČNÝCH A ZABEZPEČOVACÍCH SYSTÉMOV

PARTS OF MODEL OF INFORMATION AND SAFETY SYSTEMS

Modelovacie techniky pre rozsiahle a zložité systémy sa vyberajú s ohľadom na očakávaný výsledok modelovania. Pre rutinný postup syntézy vo väčšine prípadov postačí skúsenostný prístup. Model systému s exaktným opisom jeho atribútov vyžaduje aplikáciu niektorých teoretických záverov. Pre informačné a zabezpečovacie systémy je zvolený model, vychádzajúci z teórie informácií. Tento model možno ďalej precízovať pomocou systémovej a nakoniec obvodovej teórie. V predkladanom článku sú opísané dva nástroje aparátu teórie informácií pre spracovanie modelu systému. Ide o vyjadrenie nerovnosti pre spracovanie informácií a o kvantifikáciu chýb pri manipulácii s informáciou.

Úvod

Při analýze a syntéze informačného a zabezpečovacieho systému existujú dva základné postupy:

• pre dohodnuté funkcie sa vyberá štruktúra technických a programových prostriedkov systému na základe skúseností projektanta z predošlých aplikácií. Vyber je závislý od technologického úrovne komponentov systému a od celkovej sumy, ktorú je odberateľ ochotný zaplatiť. Úloha riadenia systému je zložená zo „standardných elementov“.

• podrobne sa specifikujú požadované funkcie systému vo vzábe na riadený systém bez ohľadu na budúcu skladbu HW a SW komponentov. V ďalšom kroku sa vytvorí model funkcie, na ktorom sa definuje úloha riadenia ako čiastková úloha riadenia principálneho procesu. Pri tvorbe modelu funkcie možno zobrať za základ niektorý z referenčných modelov, ak ide o obvyklý sortiment služieb. Pre osobitný sortiment služieb musí byť vykonaný podobný postup, ako sa používa pri tvorbe referenčných modelov. Účinným prostriedkom je vrstvenie funkcie. Tento postup umožňuje rozloženie funkcie na jednoduchšie moduly (vrstvy funkcie). Ak sa vyrieši spolupráca vrstiev, možno pri syntéze použiť postup, známy z objektového programovania. HW a SW komponenty sú vybrané tak, aby splnili ľahšie súrodé funkcie. Charakteristiky vykonávania funkcie vrstiev (časové, objemové, spoľahlivostné, bezpečnostné, ...) sú závislé od technološkých štruktúr.

Modelling techniques for large and composite systems are chosen with regard to the expected result of modelling. For routine procedure of synthesis the empirical method is sufficient in most cases. System model with exact description of its attributes demands application of some theoretical conclusions. For information and safety systems a model derived from Information theory is selected. This model can then be specified with the help of the system and, eventually, circuit theory. In the presented paper two tools of Information theory apparatus for model system processing are described. They express information processing inequality and quantification of faults occurring by information manipulation.

Introduction

When analysing and synthesising an information and safety system two ground lines exist:

• for denominated functions a structure of technical and program elements of the system is selected based on a designer’s experience from the last application. The selection depends on technology level of system components and on general sums which the customer is willing to pay. The task of system control consists of “standard elements”.

• the demanded functions of the system are thoroughly specified in connection with the controlled system regardless of the future composition of HW and SW components. In the next step the function model is created on the basis of which a control task is defined as a partial task of the primary process control. When creating a function model it is possible to use some of the reference models as a basis provided that a usual range of services is demanded. For a special range of services a similar procedure to the one used during the creation of reference models, has to be performed. The interleaving of functions is an effective tool. This procedure enables decomposition of synthesis responsibilities on simple modules (layers of the functions). Provided that the co-operation of the layers is solved, the procedure well-known from the object programming can be used in the synthesis. HW and SW components are chosen for

1University of Žilina, Faculty of Electrical Engineering, Veľký diel NF, SK-01026 Žilina, Slovak Republic,
Tel.: +421-89-5133262, Fax:+421-89-652241, E-mail: tomas@fpedas.utc.sk
2Tel.: +421-89-655559, Fax: +421-89-652241, E-mail: rastoc@fel.utc.sk
3Tel.: +421-89-655559, Fax: +421-89-652241, E-mail: zahra@fel.utc.sk
Výber nástrojov pre modelovanie úlohy riadenia

Výber modelovacích techník pre doterajšie technologické stupne informačných a zabezpečovacích systémov vychádza z skúsenostného postupu. Tento prístup pokrýva takmer všetky požiadavky na riešenie úlohy syntézy a analyzy. Išlo napríklad o modely funkcií, model dátových tokov, entitno-relačný model, protokolový model, model porúch a ďalšie modifikované modely. Tieto modely sa dajú zvládniť aj s príslušnými prepracovániami a končí špecifikáciou protokolu a stanovením príslušného formálizmu jeho konštrukciu.

Činnosť informačného aj zabezpečovacieho systému môže byť rozložená na štyri základné druhy služieb: získavanie, uchovávanie, prenos a transformácia relevantných, aktuálnych a garantovaných informácií (obr. 1). Každá z čiastkových služieb je spojená so štruktúrou HW a SW prostriedkov, ktoré vykonávajú „technológiu“ príslušných operácií. Aby systém poskytoval požadovaný sortiment služieb, musia byť elektromechanické súčasti určené do sekvencie, ktorých vykonávanie je riadené. Charakteristickým spektrom funkcií sú silne závislé aj od spoľahlivosťi riadenia. Už pri zostavovaní sekvencie čiastkových služieb musí byť zohľadnený technologický stupeň informačných služieb. Napríklad vykonnosť počítačovej siete ovplyvňuje distribuovanie a umiestnenie DB systémov, počet a interakciu aktualizácie replík DB, atď. Jadro tejto tetráki je vytvorené riadiaceho postupu, ktorý začína rozložením služieb systému na primitívy, a končí špecifikáciou protokolu a stanovením príslušného formálizmu jeho konštrukciu.

Za jadro problému analyzy a syntézy informačných a zabezpečovacích systémov s osobitným sortimentom služieb možno považovať zostavenie modelu, ktorý pokrýva celý pracovný stupeň informačných služieb a stavov systému. V predkladanom článku je pokus o jednotácnu prístup k modelovaniu takých systémov s využitím niektorých prvkov teórie informácií.
Na tomto riziku sa podieľajú všetky časti systému riadenia. Pre rozsiahle a zložité systémy by sa mali modelovacie techniky doplniť najmenej o informačný model. Informácia je pre všetky takéto systémy primárnym „substrátom“, s ktorým sa v systéme manipuluje. Informačný model má preto ambičie byť jednotiacim pre doterajšie jednoduché modely.

Zabezpečovací systém je podmnožinou informačného systému. Jeho úlohou je na riešenie problému riadenia železničnej dopravy. Pri riadení dopravného procesu možno rozlišiť tri hierarchické úrovne: procesnú, operatívnu a menežérsku. Od podopatrujúcej časti riadenia železničnej dopravy. Potom možno hovoriť o úrovni bezpečnosti pre prehliadanie a riadenie železničnej dopravy. Potom možno hovoriť o úrovni bezpečnosti pre prehliadanie a riadenie železničnej dopravy.

Zabezpečovací systém je podmnožinou informačného systému. Jeho úlohou je na riešenie problému riadenia železničnej dopravy. Pri riadení dopravného procesu možno rozlišiť tri hierarchické úrovne: procesnú, operatívnu a menežérsku. Od podopatrujúcej časti riadenia železničnej dopravy. Potom možno hovoriť o úrovni bezpečnosti pre prehliadanie a riadenie železničnej dopravy. Potom možno hovoriť o úrovni bezpečnosti pre prehliadanie a riadenie železničnej dopravy.
nosi zabezpečovacieho systému ako o miere, ktorou sa dá vyjadriť riziko nesprávneho vytvorenia a nesprávnej interpretácie tých povelov, ktoré vytvára zabezpečovací systém. Za nesprávne vytvorenie povelu sa pritom považuje aj vytvorenie povelu správnym postupom, ale na podklade nesprávnych vstupných veličín pre jeho vytvorenie. Základná schéma jednostupňového riadenia procesu je na obr. 2.

Pre úlohy analýzy a syntézy systému s definovanou úrovňou bezpečnosti treba stanoviť postupy na zaistenie správania sa systému vo všetkých jeho predvídateľných stavoch. Tieto postupy sa realizujú cez ochranné mechanizmy zabezpečovacieho systému. Ochranné mechanizmy systému musia zaistить, že aj v prípade výskytu poruchy systém vykonáva svoje funkcie presne podľa vopred definovaneho algoritmu. Opatrenia na zaistenie takéhoto správania sa systému možno aplikovať na systémovej úrovni a na úrovni funkčných jednotiek a prvkov systému. Na systémovej úrovni ide predovšetkým o voľbu vhodnej štruktúry systému. Opatrenia na úrovni funkčných jednotiek a prvkov sú zamerané najmä na detekciu poruchy a negáciu jej účinkov.

Klasifikácia chýb

Zabezpečovací systém sa podieľa na týchto operáciách schémy riadenia podľa obr. 2: • získavanie veličín V, D, R, S, • analýza veličín R, Z′, V, D, S, • tvorba veličín C, • prenos potrebných veličín medzi dvoma miestami.

Pre všetkých týchto operáciách môže vzniknúť chyba. Chyby vedú k nesprávnemu vytvoreniu riadiacej veličiny C (povelu na zmenu stavu), alebo k nesprávnej interpretácií riadiacej veličiny (prechod do nepríslušného stavu v priestore veličín S). Pre definovanie úroveň bezpečnosti treba tieto chyby klasifikovať a nájsť opatrenia na zaručenie akceptovateľného výskytu (pravdepodobnosti alebo intenzity) nezistených, alebo neošetrených chýb.

misinterpretation of the commands produced by the safety system. Commands resulting from a correct procedure but using incorrect input quantities are also considered incorrect commands. The principal scheme of the one-stage process control is shown in Fig. 2.

For the tasks of analysis and synthesis of the system with a defined level of safety the procedures ensuring the behaviour of the system in all its predictable states must be defined.

These procedures are realised through the defence mechanisms of the safety system. They have to ensure fulfilling of the demanded functions according to the pre-defined algorithm even in the case of failure. Precautions taken to ensure such system behaviour can be applied on the system level as well as on the level of functional units and system components.

On the system level the choice of the appropriate system structure is involved above all. Precautions taken on the level of functional units and components aim mainly at fault detection and negation of fault effects.

Fault Classification

The safety system takes part in the following operations of the control scheme shown in Fig. 2:

- Obtaining V, D, R, S quantities
- Analysing R, Z′, V, D, S quantities
- Producing C quantities
- Transmission of required quantities between 2 places.

A fault may occur in all of these operations. Faults result in an incorrect production of the control C quantity (the command for a change of state) or in misinterpretation of the control quantity (transition to an unauthorised state in the area of S quantities). To define the safety level these faults must be classified and precautions that can guarantee acceptable occurrence (probability or rate) of unidentified or unattended faults must be taken.
Všetky časti zabezpečovacieho systému, ktoré ziskávajú veličiny V, D, R, S, analyzujú veličiny R, Z', V, D, S, vytvárajú veličiny C a podliehajú sa na prenose všetkých veličín riadeného systému, možno takmer bez výnimky považovať za nejakú podobu konečného automatu (KA). Chyby, ktoré môžu vzniknúť v činnosti KA, možno klasifikovať do tried:

a) chyby v jazyku,
b) chyby v prenose zo stúpku na výstup KA,
c) chyby formátu,
d) chyby správania (kauzality vykonávania čiastkových funkcii),
e) chyby poskytovania služby vyššiemu systému (chyby kauzality služieb).

Na kompletnej opis systému treba zostaviť model, ktorý okrem uvedených skutočností umožní zarátať aj účinky operačného prostredia, teda kombinovať dva a viac náhodných procesov, ktoré môžu mať rozdielny charakter rozdelenia pravdepodobnosti.

Ak predpokladáme, že stavy objektu sa dajú opisť ako náhodné premenné, potom možno výhodou použiť aparát teórie informácií na vytvorenie charakteristik toku porúch (pri analýze), alebo na opis modifikácie takého toku (pri syntéze). Ide o nasledujúce časti informačnej teórie.

Definícia: Náhodné premenné

Stavy objektu ako náhodné premenné:
Nech sú stavy objektu považované za náhodné premenné X₁, X₂, ..., Xₙ. Ich vlastnosti sú dostatočne opísané funkciou rozdelenia pravdepodobnosti p(x₁, x₂, ..., xₙ). Premenné X₁, X₂, ..., Xₙ môžu byť identicky rozdelené podľa niektorého typu rozdelenia pravdepodobnosti. Môžu byť nezávislé, podmienene závislé, alebo štatisticky závislé. Pri známanom rozdelení pravdepodobnosti náhodných premenných sa dá stanoviť entropia stavov objektu.

Entropy umožňuje opisť objekt v potrebné forme, napríklad pri tvorbe kódu, ktorým je opisovaný celkový stav objektu.

Opis stavov objektu pomocou nerovností pre spracovanie dát

Prepokladajme, že stavy objektu tvoria Markovovu refaz. Nerovnosť pre spracovanie dát sa použije na demonstrácii, že žiadna „šíkovaná“ manipulácia s údajmi nemôže zlepšiť výpočet stavových charakteristik.

Definícia: Náhodné premenné X, Y, Z tvoria Markovovu refaz v tomto poradí, ak podmiene rozdelenie Z závisí len od Y a je podmienené nezávisie od X. Premenné X, Y, Z tvoria Markovovu refaz X→Y→Z, ak spoločná pravdepodobnostná funkcia sa dá nájsť takto:

\[ p(x, y, z) = p(x) \cdot p(y | x) \cdot p(z | y). \]  (1)

Z toho vyplývajú niektoré jednoduché dôsledky:

• X→Y→Z vtedy a len vtedy, ak X a Z sú podmiene niezávislé pre dané Y. Implicitne je v tom podmienné nezávislosť, pretože

All parts of the safety system that obtain V, D, R, S quantities, analyse R, Z', V, D, S, quantities produce C quantities and take part in the transmission of all the controlled system quantities can be regarded (almost without exception) as a certain kind of the finite automaton. Faults that can occur in operation of the finite automaton may be classified into the following classes:

a) Language faults
b) Faults in transmission from the input to the output of the finite automaton
c) Format faults
d) Behaviour faults (faults in causality of performing partial functions)
e) Faults in providing services to the superior system (faults in service causality).

For a complete system description we need to create a model that, apart from the mentioned facts, enables to incorporate the effects of the operational surroundings as well- thus to combine two and more random processes, which can have different character of probability distribution.

Supposing that the object states can be described as random variables, the information theory apparatus can be conveniently used to create characteristics of fault flow (during analysis) or to describe the modification of such a flow (during synthesis). The following parts of information theory are involved.

Object states as random variables
Let the object states be regarded as the random variables X₁, X₂, ..., Xₙ. Their characteristics are sufficiently described by the probability distribution function \( p(x₁, x₂, ..., xₙ) \). Variables X₁, X₂, ..., Xₙ can be identically sorted by some type of probability distribution. They can be independent, conditionally dependent or statistically dependent. When the probability distribution of the random variables is known, entropy of the object states can be estimated.

Entropy enables to describe the object in the necessary form, e.g. during the creation of the code, by which is the comprehensive object state described.

Let us suppose that object states create a Markov chain. The data processing inequality can be used to show that clever manipulation with the data cannot improve the computation of state characteristics.

Definition: Random variables X, Y, Z form a Markov chain in this order if the conditional distribution of Z depends only on Y and is conditionally independent from X. Specifically, variables X, Y and Z form a Markov chain X→Y→Z if the joint probability mass function can be written as:

\[ p(x, y, z) = p(x) \cdot p(y | x) \cdot p(z | y). \]  (1)

Some simple consequences result:
• X→Y→Z if and only if X and Z are conditionally independent for given Y. Markovity implies conditional independence because
\[
p(x, y | z) = \frac{p(x, y, z)}{p(y)} = \frac{p(x, y)p(z | y)}{p(y)} = \frac{p(x | y)p(z | y)}{p(y)} \quad (2)
\]

Takto sú charakterizované Markovove refaze, ktoré môžu byť rozšírené na definované Markovove polia. Sú to n-rozmerné náhodné procesy, v ktorých vonkajší a vnútrajší je nezávislý voči danej hranici.

- \( X \rightarrow Y \rightarrow Z \) implikuje \( Z \rightarrow Y \rightarrow X \). Tieto podmienky možno zapisovať aj takto: \( X \leftrightarrow Y \leftrightarrow Z \).
- Ak \( Z = f(Y) \), potom \( X \rightarrow Y \rightarrow Z \).

Teraz už možno dokazať dôležitú teóremu, demonštrujúcu, že žiadne spracovanie \( Y \) (deterministic alebo náhodné) nemôže zvýšiť informáciu, že \( Y \) vyprázdnil \( X \).

**Teorema 1:** Ak \( X \rightarrow Y \rightarrow Z \), potom \( I(X;Y) \geq I(X;Z) \).

\[ \text{Dôkaz: Podľa refazového pravidla môžeme rozšíriť vzťahom informáciu dvoma spôsobmi:} \]
\[
I(X;Y,Z) = I(X;Z) + I(X;Y | Z) \quad (3)
\]
\[
I(X;Y) = I(X;Y | Z) + I(Y;Z) \quad (4)
\]

Pretože \( X \) a \( Z \) sú podmienené nezávislé pre dané \( Y \), je \( I(X;Z | Y) = 0 \). Pretože \( I(Y;X | Z) = 0 \), dostávame
\[
I(X;Y) \geq I(X;Z). \quad (5)
\]

Rovnosť platí vtedy a len vtedy, ak \( I(X;Y | Z) = 0 \), t.j. \( X \rightarrow Y \rightarrow Z \) vytvára Markovovu refaz. Podobne sa dá dokazať, že
\[
I(Y;Z) \geq I(X;Z). \quad (5)
\]

**Dôsledok:** Pre vžiať prípad, ak \( Z = g(Y) \), je \( I(X;Y) \geq I(X;Z) \).

\[ \text{Dôkaz: } X \rightarrow Y \rightarrow g(Y) \text{ tvori Markovovu refaz. Funkcia } g(Y) \text{ nemôže zvýšiť informáciu o premennej } X \]

**Dôsledok:** Ak \( X \rightarrow Y \rightarrow Z \), potom \( I(X;Y | Z) \leq I(X;Z) \).

\[ \text{Dôkaz: } Z \text{ rovnice } (3) \text{ a } (4) \text{ a použitím faktu, že } I(X;Z | Y) = 0 \text{ a } I(XZ) = 0, \text{ dostávame } I(X;Y | Z) \leq I(X;Y) \]

Závislosť \( X \) a \( Y \) je zmenšená (alebo aspoň nezmenená) pozorovaním „poklesu“ náhodnej premennej \( Z \).

Všimnite si, že môže byť aj \( I(X;Y | Z) \geq I(X;Y) \) vtedy, ak \( X, Y, Z \) tvoria Markovovu refaz. Napríklad nech \( X \) a \( Y \) sú nezávislé lineárne náhodné premenné a nech \( Z = X + Y \). Potom \( I(X;Y) = 0 \), ale \( I(X;Y | Z) = H(X | Z) - H(X | Y, Z) = H(X | Z) - P(Z_{-1}) \cdot H(X | Z_{-1}) = 0.5 \ 	ext{bit} \).

**Použitie chybovej nerovnosti pre analýzu bezpečnosti**

Použitie chybovej nerovnosti je klúčové pri rozhode bezpečnosti zabezpečovacieho systému a jeho elementov. Dá sa očakávať
\[
p(x, y | z) = \frac{p(x, y, z)}{p(y)} = \frac{p(x, y)p(z | y)}{p(y)} = \frac{p(x | y)p(z | y)}{p(y)} \quad (2)
\]

This is the characterisation of Markov chains that can be extended to define Markov fields, which are n-dimensional random processes in which the interior and exterior are independent from the given values of the boundary.

- \( X \rightarrow Y \rightarrow Z \) implies that \( Z \rightarrow Y \rightarrow X \). Thus the condition is sometimes written \( X \leftrightarrow Y \rightarrow Z \).
- If \( Z = f(Y) \), then \( X \rightarrow Y \rightarrow Z \).

We can now prove an important and useful theorem demonstrating that no processing of \( Y \), deterministic or random, can increase the information that \( Y \) states about \( X \).

**Teorema 1:** If \( X \rightarrow Y \rightarrow Z \), then mutual information \( I(X;Y) \geq I(X;Z) \).

\[ \text{Proof: According to the chain rule, we can expand mutual information in two different ways} \]
\[
I(X;Y,Z) = I(X;Z) + I(X;Y | Z) \quad (3)
\]
\[
I(X;Y) = I(X;Y | Z) + I(Y;Z) \quad (4)
\]

Since \( X \) and \( Y \) are conditionally independent for the given \( Y \), \( I(XZ | Y) = 0 \). Since \( I(X;Y | Z) = 0 \), we get
\[
I(X;Y) \geq I(X;Z). \quad (5)
\]

Equality is valid if and only if \( I(X;Y | Z) = 0 \), i.e. \( X \rightarrow Y \rightarrow Z \) forms a Markov chain. Similarly can be proven that \( I(Y;Z) \geq I(X;Z) \).

**Corollary:** In specific case, if \( Z = g(Y) \), we get \( I(X;Y) \geq I(Xg(Y)) \).

\[ \text{Proof: } X \rightarrow Y \rightarrow g(Y) \text{ forms a Markov chain. Function } g(Y) \text{ cannot increase the information about variable } X. \]

**Corollary:** If \( X \rightarrow Y \rightarrow Z \), then \( I(X;Y | Z) \leq I(X;Y) \).

\[ \text{Proof: From } (3) \text{ and } (4), \text{ and using the fact that } I(XZ | Y) = 0 \text{ by Markovity and } I(XZ) \geq 0, \text{ we get } I(X;Y | Z) \leq I(X;Y) \]

Thus the dependence of \( X \) and \( Y \) is decreased (or remains unchanged) by the observation of decrease of random variable \( Z \).

Note that it is also possible that \( I(X;Y | Z) = I(X;Y) \) when \( X \) and \( Z \) do not form a Markov chain. For example, let \( X \) and \( Y \) be independent linear random variables, and let \( Z = X + Y \). Then \( I(X;Y) = 0 \), but \( I(X;Y | Z) = H(X | Z) - H(X | Y, Z) = H(X | Z) - P(Z_{-1}) \cdot H(X | Z_{-1}) = 0.5 \ 	ext{bit} \).

**Application of error inequality for analysing the safety**

The application of error inequality is key-important when analysing safety system and its components. The estimation of \( X \)
ťaž

budie chybová nerovnosť, ktorá stanovuje spodnú hranicu pravdepodobnosti chyby. Novou zložkou této myšlienku kvantifikuje.

rozšírieme dôkaz kódov s nulovou pravdepodobnosťou chyby aj na kódy s malou pravdepodobnosťou chyby. Novou zložkou bude chybová nerovnosť, ktorá stanovuje spodnú hranicu pravdepodobnosti chyby v pojmom podmienenej entropie.

Index $W$ je rovnomenne rozdelený na množine $W = \{1, 2, ..., 2^n\}$ a sekvencia $Y$ je pravdepodobnostne zväzana s $W$. Zo sekvencie $Y$ odhadujeme vyslaný index $W$. Nec je odhad $\hat{W} = g(Y)$. Definujeme pravdepodobnosť chyby

$$P(\hat{x} | x) = Pr(\hat{x} \neq x).$$

(6)

Dalej definujeme

$$E = 1, \text{ ak } (W \neq \hat{W}),$$

(7)

$$E = 0, \text{ ak sa } W = \hat{W}.$$  

Použijeme reťazové pravidlo pre entropiu na rozšírenie $H(E, W | Y)$. Dostaneme:

$$H(E, W | Y) = H(W | Y) + H(E | W, Y).$$

(8)

Pretýže $E$ je funkciou $W$ a $g(Y)$ musí byť $H(E | W, Y) = 0$. Tiež $H(E) \leq 1$, pretýže $E$ je binárná náhodná premenná. Posledný termín $H(W | E, Y)$ možno ohraničiť takto:

$$H(W | E, Y) = H(E = 0)H(W | Y, E = 0) + H(E = 1)H(W | Y, E = 1)$$

$$\leq (1 - p_E)P(E = 0) + p_E \log(1 - p_E).$$

(10)

(11)

(12)

pretože pri danom $E = 0, W = g(Y)$ a keď je $E = 1$, môžeme dostat hornú hranicu podmienejentropie. Kombinovaním týchto výsledkov dôjde k chybovej nerovnosti:

$$H(W | Y) \leq 1 + P(\hat{x} | x) nR$$

(13)

Pretýže pre prvý kód je $X(W)$ funkciou $W$, platí

$$H(X(W) | Y) \leq H(W | Y).$$

(14)

Lema: (chybová nerovnosť): Pre diskretný kanál bez památi s kódovou knihou $\xi$ a s rovnomenne rozdelenými vstupnými správami nech platí: $P(\hat{x} | x) = Pr(W \neq g(Y)).$

Potom je

$$H(X(W) | Y) \leq 1 + P(\hat{x} | x) nR.$$  

(15)

Teraz dokážeme túto lemu, ktorá ukazuje, že kapacita kanála na jeden prenos sa nezvyšuje, ak použijeme diskretný kanál bez památi viackrát.

(čosen object state) with small error probability is possible only if the conditioned entropy $H(X | Y)$ is small ($Y$ is the observed state of $X$ expressed through an intermediary, which can be a circuit output signal). Error inequality quantifies this idea.

We now extend the proof that was derived for zero-error codes to the case of codes with very small error probability. The new ingredient will be error inequality, which defines a lower boundary of the error probability in terms of the conditional entropy.

The index $W$ is uniformly distributed on the set $W = \{1, 2, ..., 2^n\}$, and the sequence $Y$ is probabilistically related to $W$. From $Y$, we estimate the index $W$ that was sent. Let the estimation be $\hat{W} = g(Y)$. Let us define the error probability

$$P(\hat{x} | x) = Pr(\hat{x} \neq x).$$

(6)

Next, we define

$$E = 1, \text{ ak } (W \neq \hat{W}),$$

(7)

$$E = 0, \text{ ak sa } W = \hat{W}.$$  

Then using the chain rule for entropies to expand $H(E, W | Y)$, we get

$$H(E, W | Y) = H(W | Y) + H(E | W, Y).$$

(8)

$$= H(E | Y) + H(W | E, Y).$$

(9)

Now, since $E$ is a function of $W$ and $g(Y)$, inevitably $H(E | W, Y) = 0$. Also $H(E) \leq 1$, since $E$ is a binary valued random variable. The remaining term, $H(W | E, Y)$, can be bounded as follows:

$$H(W | E, Y) = Pr(\hat{x} = 0)H(W | Y, E = 0) + Pr(\hat{x} = 1)H(W | Y, E = 1)$$

$$\leq 1 - P(\hat{x} | x) + P(\hat{x} | x) \log(1 - P(\hat{x} | x)).$$

(10)

(11)

(12)

since by given $E = 0, W = g(Y)$, and when $E = 1$, we can get the upper boundary of the conditional entropy. Combining these results, we obtain error inequality:

$$H(W | Y) \leq 1 + P(\hat{x} | x) nR$$

(13)

Since for a fixed code $X(W)$ is a function of $W$.

$$H(X(W) | Y) \leq H(W | Y).$$

(14)

Lema: (error inequality). For a discrete memoryless channel with a codebook (and the input messages uniformly distributed, let $P(\hat{x} | x) = Pr(W \neq g(Y))$).

Then

$$H(X(W) | Y) \leq 1 + P(\hat{x} | x) nR.$$  

(15)

We will now prove this lemma which shows that the channel capacity per one transmission is not increased if we use a discrete memoryless channel many times.
**Lema:** Nech $Y^n$ je výsledok prispôsobenia $X^n$ na diskrétny kanál bez pamäti. Potom

$$I(X^n;Y^n) \leq nC, \text{ pre všetky } p(x^n). \quad (16)$$

**Dôkaz:**

$$I(X^n;Y^n) = H(Y^n) - H(Y^n | X^n) \quad (17)$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i | Y_{1}, ..., Y_{i-1}, X^n) \quad (18)$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i | X_i) \quad (19)$$

pretože podľa definície diskrétného kanála bez pamäti. Potom

len od $X$, a je podmieneň nezávislá od všetkých ostatných. Pokračováním série nerovností je:

$$I(X^n;Y^n) = H(Y^n) - \sum_{i=1}^{n} H(Y_i | X_i) \quad (20)$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i | X_i) \quad (21)$$

$$= I(X;Y) \quad (22)$$

$$\leq nC, \quad (23)$$

kde (21) vyplýva z faktu, že entropia súboru náhodných premenných je menšia ako súčet ich individuálnych entropí. Výsledok (23) vyplýva z definície kapacity. Tým je lema dokázaná.

Teraz treba dokázat konverziu kódovacej teoremy.

**Dôkaz:** Máme ukázať, že akakolvek sekvencia $(2^{nR},n)$ kódov so $\lambda^{(n)} \rightarrow 0$ musí mať $R \leq C$.

Ak sa maximálna pravdepodobnosť chyby blíží k nule, potom priemerná pravdepodobnosť chyby pre sekvenciu kódov sa tiež blíží k nule, t.j. $\lambda^{(n)} \rightarrow 0$ implikuje $P_{e}^{(n)} \rightarrow 0$, kde $P_{e}^{(n)}$ je definovaná ako priemerná pravdepodobnosť chyby pre kód $(M,n)$: $P_{e}^{(n)} = \frac{1}{M} \sum_{i=1}^{M} \lambda_{i}$. Nech je pre každé $n$ zobrazené $W$ podľa rovnomerného rozdelenia cez $\{1, 2, ..., 2^{nR}\}$. Pretože $W$ má rovnomerné rozdelenie, je $P_{e}^{(n)} = Pr(W \neq W_{i})$.

Preto je

$$nR = H(W) = H(W' | Y^n)' + H(W | Y^n) \quad (24)$$

$$\leq H(W' | Y^n)' + I(X^n;W;Y^n) \quad (25)$$

$$\leq 1 + P_{e}^{(n)}nR + I(X^n(W);Y^n) P_{e}^{(n)} \quad (26)$$

$$\leq 1 + P_{e}^{(n)}nR + nC \quad (27)$$

Po vylúčení $n$ bude:

$$R \leq P_{e}^{(n)} R + \frac{1}{n} + C \quad (28)$$

Pre $n \rightarrow \infty$ idú prvé dva členty na pravej strane k nule a preto

$$R \leq C. \quad (29)$$

**Lema:** Ľet $Y^n$ byť výsledkom prispôsobenia $X^n$ kódu na diskrétny kanál bez pamäti. Potom

$$I(X^n;Y^n) \leq nC, \text{ pre všetky } p(x^n). \quad (16)$$

**Dôkaz:**

$$I(X^n;Y^n) = H(Y^n) - H(Y^n | X^n) \quad (17)$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i | Y_{1}, ..., Y_{i-1}, X^n) \quad (18)$$

$$= \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i | X_i) \quad (19)$$

pretože podľa definície diskrétného kanála bez pamäti. Potom

len od $X$, a je podmieneň nezávislá od všetkých ostatných. Pokračováním série nerovností je:

$$I(X^n;Y^n) = H(Y^n) - \sum_{i=1}^{n} H(Y_i | X_i) \quad (20)$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i | X_i) \quad (21)$$

$$= I(X;Y) \quad (22)$$

$$\leq nC. \quad (23)$$

kde (21) vyplýva z faktu, že entropia súboru náhodných premenných je menšia ako súčet ich individuálnych entropí. Výsledok (23) vyplýva z definície kapacity. Tým je lema dokázaná.

Teraz treba dokázat konverziu kódovacej teoremy.

**Dôkaz:** Máme ukázať, že akakolvek sekvencia $(2^{nR},n)$ kódov so $\lambda^{(n)} \rightarrow 0$ musí mať $R \leq C$.

Ak sa maximálna pravdepodobnosť chyby blíží k nule, potom priemerná pravdepodobnosť chyby pre sekvenciu kódov sa tiež blíží k nule, t.j. $\lambda^{(n)} \rightarrow 0$ implikuje $P_{e}^{(n)} \rightarrow 0$, kde $P_{e}^{(n)}$ je definovaná ako priemerná pravdepodobnosť chyby pre kód $(M,n)$: $P_{e}^{(n)} = \frac{1}{M} \sum_{i=1}^{M} \lambda_{i}$. Nech je pre každé $n$ zobrazené $W$ podľa rovnomerného rozdelenia cez $\{1, 2, ..., 2^{nR}\}$. Pretože $W$ má rovnomerné rozdelenie, je $P_{e}^{(n)} = Pr(W \neq W_{i})$.

Preto je

$$nR = H(W) = H(W' | Y^n)' + H(W | Y^n) \quad (24)$$

$$\leq H(W' | Y^n)' + I(X^n;W;Y^n) \quad (25)$$

$$\leq 1 + P_{e}^{(n)}nR + I(X^n(W);Y^n) P_{e}^{(n)} \quad (26)$$

$$\leq 1 + P_{e}^{(n)}nR + nC \quad (27)$$

Po vylúčení $n$ bude:

$$R \leq P_{e}^{(n)} R + \frac{1}{n} + C \quad (28)$$

Pre $n \rightarrow \infty$ idú prvé dva členty na pravej strane k nule a preto

$$R \leq C. \quad (29)$$
We can rewrite (28) as
\[ P(n) \geq 1 - \frac{C}{R} \cdot \frac{1}{nR}. \]
This equation shows that if \( R > C \), the error probability is moving away from 0 for sufficiently large \( n \). Hence we cannot achieve an arbitrarily low error probability at rates above capacity. This inequality is illustrated in Fig. 3. This conversion is a weak conversion of the channel coding theorem. It is also possible to prove a strong conversion, which states that for the rates above capacity, the error probability nears exponentially to 0.5. Hence, the capacity is a very clear dividing point in which the error probability is changing.

**Conclusion**

In the conclusion a procedure for description of safety from the point of dangerous error probability as a probability of random variable \( X_{ij} \) appearance is formulated. Probability \( P(X_{ij}) \) means the probability of transition of the object from state \( i \) to state \( j \). State \( X_i \) belongs to the set of safe states, state \( X_j \) belongs to the set of hazardous states. For both sets of states a more precise division can be used, by which a tree-type structure of displaying states into random variables is used.

- Safety is described by the states structure. This structure can be used to describe states of the whole object, alternatively in hierarchical order to describe the state of single elements, or object functions.
- For individual object types (safety system, or transport route as a whole) a state dependency type is determined (of the states represented by random variables). In the first approach it can be assumed, that random variables (object states) create Markov chain.
- When manipulating with random variables, facts concluding from data processing inequality have to be respected.
- The rate of object safety depends on the probability of a wrong estimation of the random variable \( X \) based on knowing the variable \( Y \). By using the error inequality the requirements for logical representation of safety functions can be estimated.

The paper was elaborated with the support of grants VEGA 1/5230/98 and 1/5255/98.

Reviewed by: P. Peniak, L. Skyva