Nakladatelství BEN Praha a VŠB-Technická universita Ostrava

Zpracováno pro seminář „Perspektivy elektroniky“ (28. – 29. 3. 2001 Rožnov p. Radhoštěm)

Moderní metody komprese a kódového zabezpečení pro multimediální komunikace

(souhrn knižní publikace)

Karel Vlček

Obsah:

V Rožnově pod Radhoštěm 2001

1. Historické počátky teorie komunikace, redundance zpráv

Všeobecně rozšířený názor o prvenství autorské publikace říká, že autorem je ten, kdo jako první publikoval důležitý poznatek. Ačkoliv je znění tohoto pravidla jednoduché, jeho použití může být komplikované. Právě taková situace nastala při publikování Hammingových kódů. První publikaci, která na Hammigovy kódy upozorňuje, napsal Shannon, který uvádí ve své práci z roku 1948 Hammingův (7,4)-kód jako příklad s odkazem na Hammingovo autorství. Potom, co si Shannonovu práci přečetl Golay, začal sám pracovat na kódech pro opravu chyb a dosáhl pozoruhodných výsledků. Kód, který objevil byl nazván Golayův (23,12)-kód. Golay přitom provedl zobecnění Hammingova (7,4)-kódu na všechny Hammingovy kódy. Obě tyto práce byly vydány před první Hammingovou prací o kódech, která vyšla až roku 1950. To byly pozoruhodné začátky, které provázely Shannonovy podnětné publikace z let 1948 a 1949. Tyto Shannonovy práce [1] a [2], ve kterých vyslovil matematicky rigorózní definici informace a formuloval věty o kompresi zpráv a o kapacitě kanálu, se staly základem oboru, který je nejčastěji nazýván *teorie komunikace*.

Na začátku padesátých let po vydání Shannonových prací zavládlo velké očekávání, které vkládalo naděje do „revoluce při praktickém uplatnění kódování“. Tyto praktické aplikace však předběhl pokrok technologický. Hlavní aplikace kódování se očekávaly v telekomunikační technice, ale právě na začátku padesátých let se podařilo dosáhnout významných zlepšení fyzikálních vlastností komunikačních kanálů v té době používaných. Díky zlepšení technologie a díky použití nových materiálů došlo v té době ke zlevnění dálkových komunikačních linek a současně ke zkvalitnění jejich parametrů. Od té doby jsou hlavní investiční náklady na výstavbu telekomunikačních sítí spojovány s problematikou spojovací, ne přenosové techniky.

Technické aplikace kódování se však překvapivě uplatnily v nové oblasti: použití hromadných pamětí počítačů. Zde je bezpečnostní kódování používáno k překlenutí nedokonalostí materiálu, který tvoří paměťové médium. Vzhledem ke stále se zvyšující hustotě magnetického i optického záznamu bude tato oblast ještě dlouhou dobu „hlavním odběratelem“ aplikací kódování zdroje i kanálového kódování. Dokladem o tomto trendu je použití vláknové optiky k přenosu a optických disků k ukládání informace. Souvisí to s vlnovou délkou světla. V důsledku toho, že vlnová délka světla je jen několik set nanometrů, je možné dosáhnout při přenosu po skleněném vlákně rychlého časového multiplexování mnoha zpráv. Informace na optickém médiu je možné zaznamenávat malými rozměry detailů, tím se dosahuje vysoké hustoty záznamu. Pro další zlevnění komunikací je využívána komprese zpráv pomocí kompresních kódů. Avšak zpráva, která obsahuje málo redundance je vlivem rušení náchylná ke ztrátě informace.

Před ztrátou informace je nutné zprávu chránit bezpečnostním kódem. Optická média jsou všeobecně náchylnější ke vzniku *shlukových chyb*. Detekce nebo korekce shlukových chyb vhodným kanálovým (bezpečnostním) kódem je náročnější než zabezpečení zpráv před ojedinělými chybami. Při konstrukci bezpečnostních kódů je v takovém případě nutné vycházet z abecedy zdroje, který používá nebinárních symbolů. Nových vlastností bezpečnostních kódů je možné dosáhnout jejich zřetězením. Komplikuje se proces kódování a dekódování, ale zlepší se vlastnosti (zřetězením nově získaného) bezpečnostního kódu. Základní rozdělení zřetězených kódů je reprezentováno dvěma odlišnými způsoby uspořádání: sériovým s vnitřním a vnějším kódem a paralelním s prokládáním, které se dále dělí podle způsobu prokládání na sériové a paralelní. Zřetězené kódy jsou v současné době předmětem intenzívního výzkumu, protože výsledné řešení je jednodušší, než by muselo být, kdyby se jednalo o použití pouze jednoho kódu s odpovídajícími vlastnostmi.

2. Zdroj zpráv bez paměti, jednotky informace, entropie zdroje zpráv

Je-li vytváření jednotlivých symbolů na výstupu zdroje informace statisticky nezávislé, je zdroj označován jako *zdroj informace bez paměti*. Je úplně popsán abecedou symbolů S a pravděpodobnostmi $P(s_1), P(s_2), P(s_3), \ldots, P(s_q)$ výskytu jednotlivých symbolů. U zdroje zpráv bez paměti je možné vypočítat průměrnou informaci. Průměrné množství informace na symbol je tedy označováno jako *entropie* $H(S)$ *diskrétního zdroje bez paměti*:

$$H(S) \hat{=} \sum P(s_i) \cdot \log_2 \frac{1}{P(s_i)} \quad [Sh / symbol] .$$

Jednou z interpretací *entropie zdroje je průměrná informace na symbol* vytvářený zdrojem. Je proto přirozené, že zkoumání bude zaměřeno na skutečnost, jak entropie závisí na různých pravděpodobnostech výskytu symbolů vytvářených zdrojem. Jinak řečeno, jak mnoho informace může zdroj vytvářet.

Pod pojmem entropie rozumí míra neurčitosti, kterou má průměrně jeden symbol zprávy. Nechť E je zpráva s pravděpodobností výskytu $P(E)$, která je vyjádřena jednotkami informace. Volba jednotky informace je dána výběrem základu logaritmu v předcházejícím vztahu. Bude-li základ logaritmu číslo 2, je jednotkou informace *shannon* [*Sh*].

$$I(E) = \log_2 \frac{1}{P(E)} \quad [Sh] .$$

Je-li použit přirozený logaritmus, bude jednotka informace *nat* (*na*tural unit):

$$I(E) = \ln \frac{1}{P(E)} \quad [nat] .$$

Při použití logaritmu o základu $a = 10$ bude jednotkou informace *hartley*. Byl to R. V. Hartley, kdo v roce 1928 poprvé použil pro vyjádření informace logaritmickou míru:

$$I(E) = \log_{10} \frac{1}{P(E)} \quad [hartley] .$$

Při komunikaci je výhodné, jsou-li jsou zprávy co nejkratší. Zestručnění zprávy bývá nazýváno různě: nejčastěji komprese (stlačení). Ve stejném smyslu se používá také pojmu komprimace (zahuštění).

Cílem zestručnění je, aby zpráva měla stejný informační obsah, ale byla přitom vyjádřena menším počtem symbolů. Pokud se však jedná o symboly vyšší abecedy, není vodítkem pouze počet symbolů. Je nezbytné provést přepočet na původní abecedu zdroje. Volba vhodného způsobu komprese bude závislá na charakteru zprávy. Jinak bude probíhat komprese textového souboru, jinak komprese obrazu nebo hlasu, či hudby. Základní výběr metody komprese spočívá v rozhodnutí, zda bude použito komprese bezztrátové nebo ztrátové.

3. Shannonova věta o kódování zdroje zpráv, komprese zpráv

Pro zdroj informace *S* platí $H(S) \le L_{\min}(S) \le H(S)+1$. Použijeme-li místo zdroje *S* zdroj S^n, můžeme napsat $nH(S) \le L_{\min}(S^n) \le nH(S)+1$, platí tedy i

$$H(S) \le \frac{L_{\min}(S^n)}{n} \le H(S) + \frac{1}{n}.$$

Pro $n \to \infty$ platí $\frac{L_{\min}(S^n)}{n} \to H(S)$.

Podle této Shannonovy věty vede komprese zprávy k hranici, která je určena hodnotou entropie. Optimální komprese dat může být dosažena právě Huffmanovou konstrukcí kódu při rozšíření zdroje S na zdroj S^n. Pojem entropie zavedl v teorii informace Shannon v roce 1948. Byl inspirován Boltzmannem, který pojem entropie zavedl ve fyzice již v roce 1896.

Metody komprese, které se nazývají bezztrátové, umožňují, aby zpráva byla obnovena v původní podobě. Metoda ztrátová, o které bude řeč v následující kapitole, to neumožňuje. Při použití ztrátové metody je zpráva po expanzi (což je postup opačný než komprese) jiná než před kompresí. Obvykle je ztrátová metoda komprese přípustná tehdy, když je možné dosáhnout výrazného zestručnění a současně nepostřehnutelných změn ve zprávě po expanzi.

Zajímavé výsledky poskytuje zkoumání nadbytečnosti přirozených jazyků. Abychom mohli popsat vlastnost zprávy analyticky, seznámíme se s definicí *redundance*. Pro vyjádření množství informace $I(u_i)$ zdrojem s abecedou u_i popsaným entropií $H(u_i)$ je nutné vytvořit zprávu o střední délce $N = \frac{I(u_i)}{H(u_i)}$ znaků. Při použití optimálního zdroje zpráv se stejnou velikostí abecedy by byla nutná jen zpráva délky $N_{\min} = \frac{I(u_i)}{H_{\max}(u_i)}$. Relativní prodloužení zprávy vytvářené neoptimálním zdrojem je vyjádřeno jako *redundance* (nadbytečnost)

4. Bezztrátová komprese, konstrukce Huffmanova kódu

Bezztrátové komprese je možné dosáhnout různými postupy, které jsou pojmenovány podle použitých způsobů optimalizace délky zpráv. Opakování je možné vypozorovat také u skupin symbolů, slov nebo částí vět přirozeného jazyka. Rozlišujeme různé postupy bezztrátové komprese:

- pravděpodobnostní (založené na pravděpodobnosti výskytu symbolů ve zprávě),
- slovníkové (při nich se sleduje v jistém plovoucím okně výskyt skupin symbolů nebo slov),
- modelováním kontextu (jejich účinnost je nejvyšší pro přirozený jazyk),
- aritmetickými metodami (s použitím násobení a dělení velkých čísel).

Ke každé skupině algoritmů bezztrátové komprese bude podána stručná charakteristika a podmínky efektivního použití. Pro hodnocení kvality komprese zprávy je možné vyjádřit kompresní poměr, který je dán délkou zprávy po kompresi k délce zprávy před kompresí. Prefixové kódování je možné vždycky jednoznačně dekódovat. Při čtení zprávy složené z prefixových kódových slov najdeme vždy nejmenší počet symbolů, které tvoří kódové slovo a ihned je můžeme dekódovat. Dekódované symboly prefixového kódování potom umažeme a zase hledáme nejmenší počet znaků tvořících kódové slovo. V angličtině se nazývají tyto kódy *"instantaneous codes"*, což lépe vystihuje jejich příznačnou vlastnost, kterou je to, že mohou být okamžitě po přijetí dekódovány. Někteří autoři doporučují český název kódy s bezprostřední rozhodnutelností. Žádný z českých názvů však nemá takovou výpovědní schopnost jako původní anglický název.

Je zřejmé, že nároky na kapacitu vyrovnávací paměti budou určeny délkou nejdelšího kódového slova, nikoliv délkou zprávy, jak by tomu muselo být, kdyby kód nebyl prefixový. Výhody prefixového kódování jsou zřejmé, proto bylo sestrojeno mnoho postupů, které umožňují vytvářet prefixové kódování. Nejznámějším postupem je tzv. Huffmanova konstrukce, která je založena na pravděpodobnosti výskytu jednotlivých slov zdrojového kódu. Huffmanovo kódování není jediným způsobem vytváření nejkratšího kódu. Je však nejefektivnějším postupem.

Huffmanův algoritmus popisuje následující postup: [konstrukce Huffmanova kódu pro jiný než binární kód je podobná, liší se pouze v bodě c)].

a) seřadíme symboly podle klesající pravděpodobnosti,

b) poslední dva symboly sloučíme do jedné dvojice. Pravděpodobnost výskytu se rovná součtu pravděpodobností symbolů, které dvojici tvoří,

c) opakujeme body a) a b) tak dlouho, až zbudou pouze dva sloučené symboly, kterým přiřadíme binární symboly 0 a 1,

d) vrátíme se o krok zpět a symbolům, které byly v daném kroku sloučeny, přiřadíme kódovou kombinaci vzniklou rozšířením kódové kombinace sloučeného symbolu zprava o jeden nebo více binárních symbolů. Kódové kombinace ostatních symbolů se v daném kroku nemění,

e) bod d) opakujeme tak dlouho, až přiřadíme kódové slovo všem zdrojovým symbolům.

5. Ztrátová komprese, H.261, JPEG, MPEG a waveletová komprese

Multimediální komunikace představují aktuální směr vývoje informačních systémů. Hlavním problémem v této oblasti je zpracování obrazu, který musí být, vzhledem k velkým objemům dat, přenášen jako zpráva podrobená kompresi. Pro tento účel se často používají i ztrátové způsoby komprese.

Vlastnosti pohyblivého obrazu jsou velmi dobře prostudovány. Barevný televizní obrazový signál (videosignál) je vytvářený podle propracovaných zvyklostí. Videosignál představuje specifický typ zprávy, u nějž jsou známy spektrální vlastnosti, je u něj možné popsat pravděpodobnosti výskytu jednotlivých bodů obrazu a další vlastnosti. Při ztrátové kompresi obrazu je důležité vycházet i ze schopností lidského zraku.

Koncepce systému byla vydána organizací CCITT (Consultative Committee International on Telegraphy and Telephony) jako doporučení označená čísly H.120 a H.130. V osmdesátých letech, kdy bylo toto doporučení již k dispozici, však nebyl žádný takový kodek v Evropě vyráběn. Ve USA a v Japonsku byly v té době používané systémy pouze přizpůsobovány uživateli. Skupina specialistů SGXV/1 začala pracovat na vývoji celosvětového standardu s přenosovou rychlostí, která je násobkem 384 kb/s. Vznikl standard H.261, jehož algoritmus vyhovoval přenosovým rychlostem pro $p \times 64$ kb/s, tedy rozsahu od 64 kb/s do 2 Mb/s. Nižší rychlosti mohly být využity pro video na úzkopásmové síti ISDN (Integrated Services Digital Network).

Návrh doporučení JPEG (Joint Photography Expert Group) je určen pro kompresi statických obrazů. Komprese je založena na kódovacím algoritmu, který je použitelný v jakémkoliv kompozitním barevném systému. Každá barevná složka je transformována pomocí diskrétní kosinové transformace (DCT) v segmentech 8×8 pixelů. Aby mohla být kosinová transformace provedena, je každý segment 8×8 pixelů zkopírován symetricky podle

os *x* a *y* s překrytím pixelů na osách. Tím se preventivně odstraní okrajové jevy, které by při kosinové transformaci vznikly v důsledku nespojitosti segmentu pixelů.

Při harmonické analýze hledáme harmonické aproximující funkce. Aby byl výraz pro aproximaci vyčíslitelný, hledáme vlnové funkce $w_k(t)$, jejichž musí být zanedbatelné pro $t \to \pm\infty$. Z praktických důvodů je výhodné, aby tento útlum probíhal se vzrůstajícím časem co nejrychleji. Ve vyjádření $x(t) = \sum_{k=-\infty}^{\infty} x_k w_k(t)$ potom každá aproximující složka $x_k w_k(t)$ přispívá k vyjádření signálu $x(t)$ pouze v určitém okolí polohy, do které je posunuta.

Jestliže u harmonické funkce byl aproximující funkcí $w(t) = e^{\frac{j2\pi t}{T}}$ vyplněn celý rozsah časové osy, u waveletů je hledanou aproximující funkcí například $\psi(t)$, která nemá pokrývat celý rozsah časové osy. Dostatečné pokrytí časové osy je dosaženo posunutím $\psi(t-k)$. S ohledem na techniku výpočtů je výhodné uvažovat takové posunutí, které je vyjádřeno výrazem:

$$\psi_{j,k}(t) = 2^{j/2}\psi\left(2^j t - k\right) = 2^{j/2}\psi\left(2^j\left(t - \frac{k}{2^j}\right)\right) = 2^{j/2}\psi\left(\frac{t - k/2^j}{2^{-j}}\right).$$

Waveletová funkce $\psi_{j,k}(t)$ se obdrží z $\psi(t)$ binární dilatací s faktorem 2^{-j} a posuvem $\frac{k}{2^j}$, který se zmenšuje úměrně se smršťováním při $j \to +\infty$ a zvětšuje úměrně s roztahováním při $j \to -\infty$ v závislosti na dilatačním faktoru 2^{-j}. Wavelet má kompaktní nosič, jestliže jeho definiční množina je ohraničená. Každou funkci lze vyjádřit pomocí waveletové řady:

$$x(t) = \sum_{j,k=-\infty}^{\infty} c_{j,k}\psi_{j,k}(t), \text{ kde } c_{j,k} = c_{j,k}(x) = \left\langle x, \psi_{j,k}\right\rangle = \int_{-\infty}^{\infty} x(t)\overline{\psi_{j,k}(t)}dt = \int x(t)\overline{\psi\left(\frac{t - k/2^j}{2^{-j}}\right)}dt$$

jsou waveletové koeficienty. Funkce ψ se také nazývá mateřský wavelet. Mateřský wavelet na daném nosiči je vytvářen z tzv. otcovského waveletu pomocí multirozkladu podle rovnice:

$$\psi(x) = \sqrt{2}\sum_n g_n \phi(2x - n), \quad g_n = (-1)^n h_{1-n}.$$

Otcovský wavelet je řešením dilatační rovnice: $\phi(x) = \sum_n h_n \phi(2x - n)$. Kompaktnost nosiče ϕ a tedy i ψ vyžaduje, aby v dilatační rovnici byl konečný počet nenulových filtračních koeficientů h_n. Požadavek ortonormality funkcí: $\phi_{m,n}(x) = 2^{-m/2}\phi\left(2^{-m}x - n\right)$ potom určuje konkrétní hodnoty h_n. Jako příklad mohou být uvedeny konkrétní hodnoty

$$h_0 = \frac{1+\sqrt{3}}{4\sqrt{2}}, \quad h_1 = \frac{3+\sqrt{3}}{4\sqrt{2}}, \quad h_2 = \frac{3-\sqrt{3}}{4\sqrt{2}}, \quad h_3 = \frac{1-\sqrt{3}}{4\sqrt{2}}.$$

Nosičem otcovského waveletu ϕ je interval [0,3], nosičem mateřského waveletu ψ je interval [-1,2]. Aby se $\psi_{j,k}$ mohly používat pro časově-frekvenční analýzu, musí být spolehlivě umístěny vzhledem časové i frekvenční ose. Těmto protichůdným požadavkům je možné vyhovět tím, že $\psi(t)$ bude mít „rychlé tlumení“. Pro případ čtyř nenulových koeficientů h_n

uvedených výše je možné vztahy pro výpočet a_k^1 a d_k^1 zapsat maticovým zápisem: $\begin{pmatrix} a^1 \\ d^1 \end{pmatrix} = \begin{pmatrix} H \\ G \end{pmatrix} a$.

6. Informační kanál, Shannonova věta o kanálovém kódování

Model symetrického binárního informačního kanálu bez paměti je nejčastěji používaným modelem nejen proto, že je jednoduchý, ale také proto, že je nejsnáze technicky proveditelný. Jeho popis je možné slovně uvést ve třech bodech:

1. Vstupní i výstupní hodnoty binárního kanálu jsou binární a jsou vyjádřeny znaky 0 a 1. Vlastnost systému bývá označována jako *homogenita*.
2. Pravděpodobnost *p*, že byla vyslána 1 a byla přijata 0, je stejná, jako pravděpodobnost, že byla vyslána 0 a přijata 1. Vlastnost systému je nazývána *symetrie*.
3. Kanál nemá paměť; to znamená, že při vyslání znaku bude pravděpodobnost bezchybného přijetí záviset pouze na tomto vyslaném znaku a nebude záviset na znacích vyslaných dříve. Tato vlastnost může být označena jako tzv. *kauzalita* (= příčinnost) kódovacího systému.

Maximální hodnota vzájemné informace $I(X,Y)$ při proměnné pravděpodobnosti vstupních symbolů se nazývá *kapacita informačního kanálu*. Kapacita informačního kanálu je veličina závislá pouze na podmíněných pravděpodobnostech kanálu. Není závislá na pravděpodobnostech vstupních symbolů, tedy na zdroji informace použitém na vstupu kanálu:

$$C = \max_{P(x_i)} I(X,Y).$$

Vzájemná informace binárního symetrického kanálu se tedy mění v intervalu od hodnoty 0 do $1 - H(p)$. Nejmenší hodnota 0 je dosažena při $\omega = 0$ nebo $\omega = 1$. Maximální hodnota $1 - H(p)$ je dosažena, když oba symboly jsou stejně pravděpodobné. Pro binární symetrický kanál s pravděpodobností chyby *p* je kapacita $C(p)$ rovna:

$$C(p) = 1 + p\log_2 p + (1-p)\log_2(1-p).$$

Shannonova věta o kódování za přítomnosti rušení říká: Uvažujme binární symetrický kanál s pravděpodobností chyby *p* a kapacitou $C(p) = 1 - H(p)$. Nechť $\varepsilon > 0$ je libovolně malé kladné číslo. Dále nechť $M = 2^{n(C-\varepsilon)}$. Potom pro dostatečně velké *n* je možné vybrat podmnožinu *M* kódových slov z 2^n všech možných tak, že pro pravděpodobnost chyby $P_{err}(K_n)$ na výstupu kanálu platí, že $P_{err}(K_n) < \varepsilon$.

Jinými slovy lze říci, že i pro špatný přenosový kanál je možné nalézt kód tak, aby zpráva byla přenesena kanálem s chybou, která dosahuje nižší úrovně chyb než je stanovená minimální hodnota.

7. Blokové kódy pro detekci chyby, zabezpečení svazku disků

Mějme dána dvě kódová slova popsaná vektory složenými ze symbolů $\boldsymbol{a} = \{a_1\ a_2\ a_3 \ldots a_n\}$ a $\boldsymbol{b} = \{b_1\ b_2\ b_3 \ldots b_n\}$. Jejich Hammingova vzdálenost je definována jako počet míst, ve kterých se hodnoty symbolů vektorů ***a*** a ***b*** liší. Píšeme:

$$d(\boldsymbol{a},\boldsymbol{b}) = \text{počet odlišností pro } i = 1, 2, \ldots, n, \text{ kdy } a_i \neq b_i .$$

Některé vlastnosti Hammingovy vzdálenosti, které můžeme odvodit z definice:

1. $d(\boldsymbol{a},\boldsymbol{a}) = 0$ a $d(\boldsymbol{a},\boldsymbol{b}) > 0$, je-li $\boldsymbol{a} \neq \boldsymbol{b}$,
2. $d(\boldsymbol{a},\boldsymbol{b}) = d(\boldsymbol{b},\boldsymbol{a})$,
3. $d(\boldsymbol{a},\boldsymbol{b}) + d(\boldsymbol{b},\boldsymbol{c}) \geq d(\boldsymbol{a},\boldsymbol{c})$ (trojúhelníková nerovnost)

pro všechna $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$, která jsou délky n.

Minimální Hammingova vzdálenost se stanovuje jako nejmenší počet odlišných symbolů dvou kódových slov daného kódu. Je zřejmé, že to má smysl pouze u kódů, které mají všechna kódová slova stejné délky, tedy u kódů blokových.

Příkladem nejjednoduššího kódu pro detekci chyby je *kód celkové parity*. Minimální hodnota kódové vzdálenosti je $d_{\min} = 2$.

K četným aplikacím bezpečnostních kódů byla v roce 1987 připojena metoda zápisu informací do několika diskových jednotek. Místo sekvenčního zápisu, který je obvyklý při použití jedné diskové jednotky, je informace do diskového pole zapisována současně do n diskových jednotek. Činnost vnější paměti se tím zrychlí asi n-krát. Kromě toho však je možné zlepšit spolehlivost diskové paměti použitím zabezpečovacího kódu.

Metoda současného zápisu informace na několik disků byla navržena před deseti lety na Universitě v Berkeley. Byla pojmenována RAID (Redundant Array of Inexpensive Discs). Metoda přinesla několikanásobné zvýšení rychlosti zápisu a čtení informací ve srovnání s použitím jednoho disku. Navíc však přinesla zlepšení spolehlivosti diskové paměti za cenu poměrně malé redundance. Ke každé skupině disků se totiž přidává pouze jeden disk jako záložní. Této výhodné vlastnosti se používá v šesti základních konfiguracích diskových polí. Podle toho jsou nazývány i metody v podrobnější specifikaci jako RAID 0 až RAID 5.

8. Blokové kódy pro korekci jedné chyby, rozšířené kódy

Hammingův kód je důležitým lineárním binárním kódem se schopností opravy chyb. Jeho vlastnosti jsou dány kódovou vzdáleností $d_{\min} = 3$. (Vznikají tedy výběrem jedné osminy slov z přirozeného binárního kódu.) Kód s minimální vzdáleností 3 detekuje až dvojnásobnou chybu nebo opravuje jednonásobnou chybu.

Hammingovy kódy se snadno dekódují a jsou *perfektní*, t.j. mají nejmenší myslitelnou redundanci. Jestliže počet kontrolních bitů m roste po jedné, je celková délka Hammingových kódů $n = 2^m - 1$, takže dostáváme binární (3,2)-kód, (7,4)-kód, (15,11)-kód, atd.

m	2	3	4	5	6	...
n	3	7	15	31	63	...
k	1	4	11	26	57	...

Tab.: 7.1 Konfigurace Hammingových kódů

Informační poměr roste rychle k 1, např. pro kód délky $2^6 - 1 = 63$ je informační poměr

$$\frac{63-6}{63} > 0{,}9.$$

Postup, který umožňuje opravovat chyby, je založen na tom, že pravděpodobnost jedné chyby je mnohem vyšší, než pravděpodobnost více chyb v jednom kódovém slově. Jedna chyba způsobí, že chybné slovo bude mít od kódového slova vzdálenost 1. Ztráta informace jednoho bitu v kódovém slově se dá opravit. Chybné slovo způsobí, že součin kontrolní matice a přijatého slova, které je transponováno na sloupcový vektor, bude nenulový.

Kontrolní matici rozšířeného Hammingova kódu získáme z kontrolní matice Hammingova kódu tak, že ke každému řádku přidáme paritní bit sudé parity a do kontrolní matice doplníme řádek jedniček. Kontrolní matice pro rozšířený Hammingův (8,4)-kód má tvar:

$$H_4 = \begin{bmatrix} & & & & & & & 0 \\ & & & H_3 & & & & 0 \\ & & & & & & & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

kde H_3 je kontrolní matice Hammingova (7,4)-kódu. Při konstruování kódových slov rozšířeného Hammingova (8,4)-kódu postupujeme následovně: rozšíříme kanonický tvar kontrolní matice Hammingova (7,4)-kódu podle předchozího schématu a úpravou, která spočívá v přičtení prvních tří řádků ke čtvrtému řádku dostaneme kanonický tvar kontrolní matice rozšířeného Hammingova (8,4)-kódu.

9. Blokové kódy pro korekci více chyb v jednom kódovém slově

Reedovy-Mullerovy kódy jsou lineární kódy definované nad $GF(2)$, které mohou být dekódovány jednoduchou technikou rozhodování. Z těchto důvodů jsou Reedovy-Mullerovy kódy důležité i přesto, že někdy nesplňují nejmenší kódovou vzdálenost. Pro každé celé m a pro každé celé r menší než m je Reedův-Mullerův kód blokovým kódem o délce 2^m a nejmenší kódové vzdálenosti $d_{\min} = 2^{m-r}$.

Přecházející podmínky zajišťují, že řádky generující matice G obsahuje pouze řádky lineárně nezávislé. Reedův-Mullerův nultého řádu je (n,1)-kód. Jedná se o jednoduchý opakovací kód. Jeho dekódování se provádí pomocí majoritního rozhodování. Reedovy-Mullerovy kódy jsou binární kódy, které jsou zobecněním dosud probíraných kódů. Jsou to speciální binární kódy délky $n = 2^m$. Kódová slova jsou tedy s výhodou popisována jako booleovské mnohočleny m proměnných. Na základě vlastností booleovských mnohočlenů jsou definovány Reedovy-Mullerovy kódy. Množina $R(r,m)$ všech booleovských mnohočlenů m proměnných stupně nejvýše r se nazývá Reedovým-Mullerovým kódem stupně r a délky 2^m.

Reedovy-Mullerovy kódy byly objeveny v roce 1954. Jejich význam spočívá v jednoduché implementaci rekurzívních algoritmů dekódovací metody. Algoritmus dekódování se snadno implementuje pomocí programu mikropočítače. R-M kódy jsou používány i v nových konstrukcích systémů průmyslové elektroniky například pro zabezpečený přenos informace drážních systémů, kde je požadována oprava dvou chyb při přenosu zpráv.

Významným přínosem R-M kódů je jejich zobecňující platnost například při odvozování tzv. duálních kódů. Duální kód je takový lineární kód, u kterého jsou vyměněny

generující a kontrolní matice. Duální kód je jiný název pro ortogonální doplněk kódu. Je to tedy kód $K^{\perp}$, jehož všechna slova jsou ortogonální ke slovům kódu K.

10. Struktura konečných těles, cyklické kódy, systematické kódování

Cyklické kódy umožňují nejúspornější implementační řešení kódového systému. V této kapitole je výklad zaměřen na cyklické kódy pro opravu jedné chyby v kódovém slově blokového kódu. Následující 10. kapitola je věnována binárním BCH kódům a další pak RS kódům. Pro všechny tyto kódy je potřebná teorie cyklických kódů, která je založena na výpočetních operacích s mnohočleny a jejich kořeny.

Matematická teorie cyklických kódů je založena na popisu vlastností konečných těles. Tato teorie přináší metodiku implementace, která je nenahraditelným nástrojem při návrhu kódů pro opravu vícenásobných a shlukových chyb, ale užitečná je i u kódů pro opravu jedné chyby v přijatém slově. Nejdříve budou uvedeny základní definice a věty a posléze i krátká diskuse o *grupách* a *konečných tělesech*.

Konečné binární těleso se šestnácti prvky $GF(16)$ je možné popsat mnohočleny. Je přirozené, že 0000 odpovídá nulovému mnohočlenu a 1000 mnohočlenu 1. Další čtveřice odpovídají mnohočlenům stupně menšího než číslo 4 s koeficienty 0 a 1. To znamená, že 0100 odpovídá x, 0010 je x^2 a 0001 je x^3. Pro tyto čtveřice je definována operace sčítání a operace násobení. Můžeme tedy násobit mnohočlenem x i jeho mocninami.

Při popisu kódu pomocí mnohočlenu budeme používat pro indexy čísla celá nezáporná. Kódové slovo tedy bude značeno posloupností symbolů $v_0 v_1 v_2 \ldots v_{n-1}$, neboť vyjádření pomocí mnohočlenu pak má u jednotlivých členů shodné indexy a exponenty proměnné veličiny mnohočlenu. Použití násobení mnohočlenů, popisujících kódová slova, usnadní popis kódů. Nové vlastnosti, které můžeme odvodit na základě znalostí operací s mnohočleny, umožňují nalézt nové vlastnosti vhodné pro tzv. snadné dekódování.

Hlavní výhodou výpočtu kódových slov cyklických kódů je to, že nyní můžeme používat operací sčítání (odečítání) mnohočlenů i jejich násobení a dělení podle početních pravidel platných pro danou číselnou soustavu.

Kontrolní matice *H* tedy obsahuje všechny mocniny mnohočlenů $GF(16)$:

$$H = \left[\alpha^{14} \quad \alpha^{13} \quad \alpha^{12} \quad \alpha^{11} \quad \alpha^{10} \quad \alpha^{9} \quad \alpha^{8} \quad \alpha^{7} \quad \alpha^{6} \quad \alpha^{5} \quad \alpha^{4} \quad \alpha^{3} \quad \alpha^{2} \quad \alpha^{1} \quad 1\right].$$

Rozepsáním koeficientů do sloupců matice je získána kontrolní matice cyklického Hammingova (15,11)-kódu:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

Mnohočlen $s^{(1)}(x)$ je získán z $s(x)$, který je obsažen v posuvném registru dělicího obvodu po dělení přijatého slova mnohočlenem $g(x)$, posuvem informace v registru dělicího obvodu, ale na vstupu dělicího obvodu přitom nesmí být žádná další informace. K tomu, aby mohla být provedena oprava, slouží zmíněný Meggittův dekódovací algoritmus. Meggittův dekodér cyklického kódu s generujícím mnohočlenem $g(x)x^4 + x^3 + 1$ je sestaven z obvodu

pro dělení generujícím mnohočlenem, obvodu pro vytvoření opravného signálu dekódováním syndromu 1000 a vyrovnávací (FIFO) paměti z patnácti klopných obvodů.

11. BCH kódy, (15,7)-kód, Meggitův dekodér pro opravu dvou chyb

Konstrukce BCH kódů zaujímá důležité místo jak v teorii, tak i v praxi. Existuje pro to více důvodů. Prvním důvodem je relativně malá délka slova těchto blokových kódů vzhledem k jejich schopnostem opravovat plánovaný počet chyb. Důvodem je i relativně snadná implementace kódových systémů BCH-kódů. Dalším důvodem pro intenzívní výzkum a realizace kódových systémů je prakticky velmi rozšířená implementace kodérů a dekodérů nebinárních BCH kódů: Reedových-Solomonových kódů (RS kódů).

Jako praktický příklad aplikace teoretických poznatků je uvedena konstrukce binárního BCH kódu o délce 15 bitů. Z důvodu návaznosti na předchozí výklad je použito postupu, který vychází z konstrukce kontrolní matice cyklického kódu pro opravu jedné chyby. Kontrolní matice je opět popisována pomocí mocnin generujících kořenů. Konstrukce kontrolní matice pro BCH kód délky 15 je zvolena proto, že v příloze D již byla popsána konstrukce konečného tělesa $GF(2^4)$, uvedený postup ale může být proveden obecně pro těleso $GF(2^m)$.

Při návrhu kódů pro opravu jedné chyby v kódovém slově byl z generujících kořenů odvozen generující mnohočlen kódu. Jeho vlastnosti jsou shodné s vlastnostmi minimálního mnohočlenu. Jestliže jsou známy generující kořeny kódu, je generující mnohočlen součinem minimálních mnohočlenů generujících kořenů.

Lze dokázat, že jestliže α je prvočíslo, je takovou soustavou: $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$. Přijetím tohoto předpokladu je volba $g(x)$ omezena na tyto prvky jako nuly. Při délce kódového slova $n = q^m - 1$ je pro daná m a t počet opravovaných chyb určen následujícím postupem:

1. Je zvolen primitivní mnohočlen stupně m a zkonstruováno konečné těleso $GF(q^m)$.
2. Jsou nalezeny minimální mnohočleny $f_j(x)$ pro α^j, kde $j = 1, \ldots, 2t$.
3. Potom $g(x) = LMC[f_1(x), f_2(x), \ldots, f_{2t}(x)]$.

Kontrolní matice H kódu pro opravu dvou chyb bude obsahovat dva řádky. Prvním řádek jsou mocniny generujících kořenů $\alpha^i, i = 0, 1, \ldots, n-1$, což je podmínkou vzniku cyklického kódu, druhý řádek je dán funkcí s argumentem generujících kořenů $f(\alpha^i)$ tak, aby rovněž vyhovoval podmínce cyklického kódu.

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \ldots & \alpha^{13} & \alpha^{14} \\ f(1) & f(\alpha) & f(\alpha^2) & f(\alpha^3) & f(\alpha^4) & \ldots & f(\alpha^{13}) & f(\alpha^{14}) \end{bmatrix}.$$

Čísla $\alpha^i, i = 0, 1, \ldots, n-1$ tedy představují čtveřice binárních číslic. Další čtveřice binárních číslic $f(\alpha^i)$ mají být voleny tak, aby mohly být dekódovány dvě chyby v každém slově kódu. Při vynásobení přijatého slova se dvěma chybami s kontrolní maticí H vznikne matice syndromu S pro chyby ve sloupcích $i = 0, 1, \ldots, n-1$ a $j = 0, 1, \ldots, n-1$. Platí:

$$S = \begin{bmatrix} \alpha^i + \alpha^j \\ f(\alpha^i) + f(\alpha^j) \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}.$$

Syndrom je tedy vyjádřen pomocí $s_1 = \alpha^i + \alpha^j$ a $s_2 = f(\alpha^i) + f(\alpha^j)$, kde *i* a *j* jsou ve vztahu k poloze chyb. Výběr funkce $f(\alpha^i)$ má umožňovat výpočet hodnot *i* a *j*. Bude-li $f(\alpha^i) = \alpha^i$ pro všechna *i*, nebudeme moci soustavu rovnic $s_1 = \alpha^i + \alpha^j$ a $s_2 = \alpha^i + \alpha^j$ vyřešit. Nabízí se možnost použít jako funkci $f(\alpha^i)$ mocninu čísel α^i a α^j. Bude-li $f(\alpha^i) = \alpha^{2i}$ pro všechna *i*, bude $s_1 = \alpha^i + \alpha^j$ a $s_2 = \alpha^{2i} + \alpha^{2j}$. Ale v binárním tělese platí $\alpha^{2i} + \alpha^{2j} = (\alpha^i + \alpha^j)^2$, takže $s_2 = (\alpha^i + \alpha^j)^2 = s_1^2$ a *i* a *j* rovněž nemohou být vyřešena.

Další volba funkce *f* může být $f(\alpha^i) = \alpha^{3i}$ pro všechna *i*. Potom soustava rovnic o neznámých *i* a *j* je následující: $s_1 = \alpha^i + \alpha^j$ a $s_2 = \alpha^{3i} + \alpha^{3j} = (\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^i\alpha^j + \alpha^{2j})$, takže po úpravě, při níž předpokládáme, že $i \neq j$ píšeme rovnici

$$\frac{s_2}{s_1} = \alpha^{2i} + \alpha^i\alpha^j + \alpha^{2j} = s_1^2 + \alpha^i\alpha^j .$$

Pro výpočet *i* a *j* jsou úpravou získány rovnice $\alpha^i + \alpha^j = s_1$ a $\alpha^i\alpha^j = \frac{s_2}{s_1} - s_1^2 = \frac{s_2}{s_1} + s_1^2$. Čísla α^i a α^j jsou kořeny normované kvadratické rovnice $x^2 + (\alpha^i + \alpha^j)x + \alpha^i\alpha^j = 0$. Při hledání *i* a *j* pomůže rozklad na kořenové součinitele ve tvaru $(x + \alpha^i)(x + \alpha^j) = 0$.

Konstrukce šestnácti čtveřic binárních čísel tělesa $GF(16)$ je provedena tak, že platí násobení a sčítání. To je podmínka pro to, aby kód mohl být cyklickým kódem. Násobení je usnadněno vyjádřením mocnin α, proto je uspořádání šestnácti čtveřic provedeno podle těchto mocnin. Vznikne matice H:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \ldots & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & (\alpha^2)^3 & (\alpha^3)^3 & (\alpha^4)^3 & (\alpha^5)^3 & \ldots & (\alpha^{13})^3 & (\alpha^{14})^3 \end{bmatrix}.$$

Po úpravě při rovnosti $\alpha^{15} = 1$, $\alpha^{18} = \alpha^3$, ..., $\alpha^{42} = \alpha^{12}$ je uspořádání kontrolní matice:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \ldots & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \ldots & \alpha^9 & \alpha^{12} \end{bmatrix}.$$

Dekódování a nalezení chyb pomocí syndromu je dosaženo vynásobením kontrolní matice *H* a přijatého slova. BCH kódy jsou definovány jako zobecnění Hammingových kódů: zatímco pro jednu chybu má kontrolní matice *H* jeden řádek [nad Galoisovým tělesem GF(16)], pro dvě chyby má dva řádky.

Obvodová implementace řešení, které poskytuje matice, by vedla k rozsáhlému obvodu. Využitím cyklických vlastností kódu je možné nalézt řešení obvodově úspornější, pokud nevadí delší doba zpracování při dekódování a opravě chyb. Takovým řešením je Meggittův dekodér. Použití Meggittova teorému pro opravu dvou chyb v přijatém slově vyžaduje úpravu přijatého slova vynásobením mnohočlenem x^8. Tím je dosažena možnost odstranění syndromu, který vyznačuje polohu chybného bitu.

12. Cyklické kódy s vyššími abecedami, zabezpečení CD záznamů

Důležitou a známou třídou BCH-kódů jsou Reedovy-Solomonovy kódy (RS-kódy), které používají vyšší abecedu zdroje. Jsou to BCH kódy, pro jejichž délku slova platí $n = q^m - 1 = q - 1$. To znamená, že $m = 1$, tedy těleso symbolů $GF(q)$ je stejné jako těleso lokátorů chyb $GF(q^m)$. Minimální mnohočlen prvku β je $f_\beta(x) = x - \beta$. Protože těleso symbolů a těleso lokátorů chyb je stejné, jsou všechny minimální mnohočleny lineární. Symboly RS-kódu jsou v informačním kanálu obvykle vyjádřeny svými binárními ekvivalenty.

Shluková chyba je působena společným vlivem. Chybné bity jsou tedy korelovány, mají společnou příčinu a musejí být opravovány jako shluk chyb. Při poruše, která způsobí shlukovou chybu (burst-error), je možné zachytit případně opravit symbol vyšší abecedy. Pro tento účel jsou vhodné právě RS kódy. RS-kódy se často používají pro zabezpečování diskových magnetických i optických pamětí. Jako příklad kanálu s výskytem shlukových chyb může nejlépe sloužit optická digitální záznamová technika známá pod názvem kompaktní disk (CD). Paměťové medium pro zvukový záznam na kompaktní disk je plastový kotouč s průměrem 120 mm, tloušťkou 1,2 mm a roztečí záznamových stop 1,6 μm. Při přehrávání je informace z disku čtena koherentním optickým paprskem rychlostí 1,25 m/s. Ve spirální záznamové stopě na disku jsou značky, které jsou nazývané „jamky“ (pits) a plochá místa mezi jamkami nazývané „země“ (lands).

Číslicový zvukový signál je zaznamenán v uspořádání délek „jamek“ a „zemí“. Symbol „1“ je představován přechodem z „jamky“ na „zem“ nebo naopak, zatímco symbol „0“ je zaznamenán jako setrvání bez přechodu. S ohledem na malé rozměry jamek jsou používané u kompaktních disků RLL-kódy (Runlength-Limited Codes), které mají omezenou délku. Hlavním zdrojem chyb na kompaktních discích jsou nedokonalosti vzniklé při výrobě disků, jako jsou bublinky v plastovém materiálu, nepřesnosti ve tvaru jamek nebo otisky prstů, škrábance, prach, špína a povrchová poškození. Protože každá jamka je asi 0,5 μm široká a dlouhá od 0,9 do 3,3 μm, chyby v kódu se projevují jako shlukové chyby, protože rušivé vlivy zasahují větší množství informačních bitů. Pro paměťový přenosový kanál je tedy nutné použít model kanálu se shlukovými chybami.

13. Konvoluční kódy, Viterbiho algoritmus, Wynerův-Ashův (8,7)-kód

Konvoluční kodéry naproti tomu lze popisovat jen jako *zdroje zpráv s pamětí.* Konvoluční kódy jsou předpisem pro kódový systém, který generuje kódová slova na základě obsahu rámce několika vstupních slov. To jakým způsobem bude zakódována určitá informační posloupnost tedy závisí nejenom na aktuální vstupní informační posloupnosti, ale také na *m* předchozích vstupních informačních slovech.

V knize jsou popisovány nejdříve konvoluční kódy pomocí generujících polynomů a generujících matic. Pak jsou rozebrány postupy dekódování, které umožňují provádět opravu chyb. Nejznámějším postupem je tzv. Viterbiho algoritmus. Po přijetí celé zprávy má být kodér v nulovém stavu. Jeho přijatá cesta určuje hledanou posloupnost. U každého stavu jsou vyznačeny minimální vzdálenosti v daném okamžiku dekódování. Cestě s minimální vzdáleností odpovídá správná posloupnost zdrojových znaků. Viterbiho algoritmus poskytuje nejpravděpodobnější odhad vyslané zprávy až po přijetí celé zprávy.

14. Turbo kódy a jejich aplikace v radiových přenosech dat

Turbo-kódy jsou vytvářeny několika paralelně zřetězenými kodéry pro generování konvolučních kódů, které jsou odděleny tzv. prokladem informací zprávy (interleaver). Dekodér je tvořen zřetězením dvou nebo více modulů popisovaných jako SISO (Soft-Input Soft-Output) bloky, které jsou rovněž navzájem propojeny bloky pro proklad (interleaver) a zpětný proklad (deinterleaver) informace ve zprávě. Moduly dekodéru spolupracují podle iterativního algoritmu, při kterém dochází k výměně dílčích výsledků dekódování mezi SISO bloky. Dekodér je v tomto uspořádání schopen se přiblížit, při dlouhých posloupnostech prokladu informace, hodnotám velmi blízkým limitní kapacitě kanálu.

V textu je vysvětlen základní princip turbo-kódů včetně řízení vlastností kódu, analýzy a zlepšování mezních parametrů návrhu základních kodérů a bloku prokladu informace ve zprávě. Základem účinnosti dekodéru je algoritmus iterativního dekódování. Další principy zřetězení a použití prokladu, které zahrnuje sériové a hybridní zřetězení dekodérů je uváděno v souvislosti s typickými hodnotami využití limitních hodnot kapacity informačního kanálu. Turbo-kódy jsou intenzívně zkoumány v souvislosti s použitím komunikace s omezeným výkonem zdroje zpráv (space communication). Téměř hotov je nový standard pro kódování telemetrických spojů. Doporučení pro CCSDS, pro ATM i pro bezdrátové aplikace, pro kanály s velkým únikem, s digitálním satelitním přenosem a pro další aplikace digitálních komunikací jsou ve velmi pokročilém stádiu příprav. Turbo-kódy představují novou třídu kódů pro kódové zabezpečení, jejichž dekódování je řešeno praktickou implementací.

Dekodér konvolučního kódu pracuje tak, že hledá nejpravděpodobnější posloupnosti bitů v kódové posloupnosti, která je porušena chybami. Tzv. Viterbiho algoritmus řeší teno úkol s nejvyšší mírou pravděpodobnosti.

$$\hat{m} = \arg\left\{\max_{m} P\left[m|y\right]\right\}.$$

Symbol $\hat{m}$ představuje posloupnost bitů, která je získána z přijaté posloupnosti y. Rovnice je řešena například pomocí Viterbiho algoritmu. Je tím získána maximálně pravděpodobná přijatá posloupnost ML (Maximal Likelihood).

15. Modelování kódových systémů pomocí VHDL jazyka

V roce 1987 byl přijat jazyk VHDL jako standard IEEE pod číslem 1076-1987. Byl rychle akceptován, protože řešil v té době již neúnosnou situaci, kterou je možné popsat jako velké množství vzájemně neslučitelných jazyků pro popis obvodů. VHDL se tedy stal standardem de jure. Nedostatkem tehdejšího provedení VHDL bylo, že byl příliš popisně zaměřený. Toho si byli výrobci číslicových obvodů vědomi. Proto pracovali na zdokonalení „vyjadřovacích prostředků“ jazyka.

V roce 1992 byla přijata inovace standardu IEEE 1076-1992. Přitom byla provedena podstatná revize jazyka, který byl uveden na trh s letopočtem 1993. V současné době opět probíhají závěrečné úpravy inovované verze VHDL tentokrát s letopočtem 1997. Tato nová verze jazyka má název VHDL-AMS (VHDL-Analogue & Mixed Signals) a obsahuje již i prostředky pro návrh analogových a smíšených - mixed (analogových-číslicových a číslicových- analogových) obvodů. VHDL je soubor prostředků, které usnadňují návrh a zvyšují kvalitu navrženého obvodu. V tomto procesu mají nesporný význam i návrhové prostředky BSDL, které byly navrženy jako doplněk standardu VHDL pod označením IEEE 1076-1987 B.