

Name index

- Aczél, J., 12, 13, 461
 Ahlswede, R., x, 78, 80, 103, 106, 139, 163,
 225, 226, 227, 233, 234, 235, 236, 237, 238,
 239, 271, 286, 290, 291, 297, 302, 303,
 343, 344, 345, 346, 348, 352, 353, 374,
 375, 376, 394, 395, 399, 447, 452, 459,
 461–462
 Amari, S., 47, 463
 Anantharam, V., 453, 460, 469
 Arimoto, S., 131, 165, 172, 463
 Arutunjan *see* Haroutunian
 Audenaert, K. M. E., 43, 463
 Augustin, U., 165, 297, 463
- Barg, A., 174, 463
 Barron, A. R., 60, 463
 Bártfai, P., x
 Beck, J., x
 Bennett, C. H., 456, 459, 463
 Berge, C., 102, 207, 463
 Berger, T., 119, 129, 140, 143, 399, 463, 468
 Bergmans, P. P., 374, 399, 459, 463
 Berlekamp, E. R., 161, 168, 169, 172, 175, 177,
 181, 183, 463, 474
 Berlin, P., 182, 463
 Berrou, C., 106, 463
 Bierbaum, M., 288, 463
 Blackwell, D., 183, 225, 227, 231, 235, 238, 239,
 383, 463
 Blahut, R. E., 32, 131, 143, 160, 168, 174, 175, 183,
 271, 463, 464, 472
 Blinovskiy, V., 233, 464
 Bloh, E.L., 70, 464
 Blokhuis, A., 205, 464
 Boë, J. M., 60, 464
 Bollobás, B., 204, 206, 464
 Boltzmann, L., 14, 32, 464
 Brassard, G., 456, 459, 463
 Breiman, L., 183, 225, 227, 231, 235, 238, 239, 463
 Brightwell, G., 207, 464
 Burnašev, M. V., 104, 182, 464
- Carathéodory, C., 310, 363
 Cai, N., 235, 291, 462
 Calderbank, R. A., 204, 205, 206, 207, 233, 464
 Carleial, A. B., 300, 303, 464
 Carter, J. L., 11, 464
 Čencov, N. N., 46, 464
 Červonenkis, A. Y., 79, 475
 Césari, Y., 60, 464
 Chan, C., 455, 464
 Chaundy, T. W., 13, 464
 Chernoff, H., 168, 464
 Cohen, G., 208, 464
 Cover, T. M., xi, 37, 59, 266, 271, 300, 303, 371,
 374, 381, 399, 459, 464, 465, 473
 Crépeau, C., 463
 Csibi, S., x
 Csiszár, I., i, 15, 27, 31, 32, 33, 44, 46, 59, 64, 65,
 66, 67, 70, 104, 129, 131, 142, 163, 165,
 166, 168, 177, 178, 179, 183, 208, 226,
 228, 234, 266, 267, 268, 270, 271, 353, 399,
 447, 452, 454, 455, 458, 459, 460, 462,
 465, 466
 Cybakov, B. S. *see* Tsybakov, B. S.
- Daróczy, Z., 12, 13, 461, 466
 Davisson, L. D., 68, 70, 131, 139, 466, 472
 Dobrušin, R. L., 32, 103, 119, 143, 180, 183,
 239, 466
 Dueck, G., 106, 162, 165, 285, 301, 459, 462, 466
 Dyačkov, A. G., 179, 180, 466
- Eggleston, H.G., 353, 466
 El Gamal, A. A., 374, 377, 379, 399, 467
 Elias, P., 11, 98, 104, 176, 179, 183, 467
 Erdős, P., 13, 205, 467
 Ericson, T., 228, 467
 Erokhin, V. D., 116, 467
- Fachini, E., 464
 Faddeev, D. K., 13, 467
 Fairthorne, M., 464
 Falk, F., 47, 467

- Fannes, M., 32, 467
 Fano, R. M., 43, 47, 50, 65, 70, 95, 105, 183, 467
 Farkas, L., xi
 Fedotov, A., 44, 467
 Feinstein, A., 105, 106, 467
 Fekete, M., 208, 467
 Feller, W., 26, 65, 73, 467
 Fenchel, W., 353, 467
 Fisher, R. A., 14, 467
 Fitingof, B. M., 70, 467
 Forney, G. D., 176, 182, 183, 467
 Forte, B., 13, 461, 467
 Frankl, P., 464
 Fredman, M., 176, 468
 Fujishige, S., 46, 468
 Fulkerson, D. R., 143, 468
 Füredi, Z., 467
- Gardner, N. T., 300, 468
 Gabidulin, E. M., 98, 468
 Gács, P., x, 80, 103, 271, 343, 345, 346, 352, 353, 394, 399, 459, 462, 468
 Gallager, R. G., 47, 106, 117, 129, 130, 131, 161, 162, 166, 167, 168, 169, 172, 173, 174, 175, 177, 178, 179, 183, 266, 268, 352, 374, 468, 474
 Gallai, T., 102
 Galluccio, A., 206, 468
 Garg, H. K., 298, 470
 Gargano, L., 206, 208, 468
 Gelfand, S. I., x, 236, 383, 396, 399, 468
 Gerrish, A. M., 129, 468
 Gibbs, J. W., 46, 468
 Gilbert, E. N., 62, 80, 160, 175, 468, 469
 Glavieux, A., 106, 463
 Gohari, A. A., 453, 460, 469
 Goppa, V. D., 100, 183, 469
 Graham, R. L., 464
 Gray, R. M., 139, 348, 375, 392, 399, 469, 472
 Greco, G., 207, 469
 Gubner, J., 291, 469
- Haemers, W., 101, 469
 Hajnal, A., 102, 467, 469
 Hamming, R. W., 79, 469
 Han, T. S., 106, 267, 271, 297, 469, 473, 476
 Hardy, G. H., 44, 469
 Haroutunian, E. A., 180, 183, 271, 469
 Harper, L. H., 78, 469
 Harremoës, P., 44, 467
 Hartley, R. V. L., 14, 469
 Hoeffding, W., 29, 30, 44, 469
 Horibe, Y., 43, 469
 Horstein, M., 182, 469
 Hu Guo-Ding, 46, 469
 Huffman, D. A., 58, 469
 Hughes, B., 233, 469
- Impagliazzo, R., 456, 469
 Itoh, K., 182, 476
- Jahn, J. H., 291, 469
 Jeffreys, H., 44, 470
 Jelinek, F., 32, 63, 118, 130, 143, 174, 470, 475
 Jerohin, V. D. *see* Erokhin, V. D.
 Jiang, J., 298, 470
- Karamata, J., 12, 470
 Karlin, S., 129, 211, 222, 231, 442, 470
 Karmažin, M. A., 99, 470
 Karush, J., 59, 470
 Katona, G. O. H., 61, 64, 67, 70, 78, 208, 462, 465, 470
 Kawabata, T., 46, 470
 Kemperman, J. H. B., 44, 165, 470
 Kesten, H., 165
 Kiefer, J., 225, 470
 Kim, Y. H., 399, 467
 Kobayashi, K., 271, 297, 469
 Kóli, T., xi
 Kolmogorov, A. N., 65, 470
 Komjáth, P., 467
 Komlós, J., x, 66, 176, 465, 468
 Korn, I., 167, 470
 Körner, J., i, 80, 100, 102, 105, 141, 142, 143, 162, 163, 165, 166, 176, 183, 205, 206, 207, 208, 226, 266, 267, 270, 271, 343, 344, 345, 346, 348, 350, 352, 353, 371, 372, 374, 375, 376, 384, 386, 388, 389, 390, 391, 394, 395, 399, 459, 462, 464, 465, 466, 468, 470, 471
 Košelev, V. N., 266, 471
 Kraft, L. G., 58, 471
 Kramer, G., 300, 303, 399, 471
 Krause, R. M., 59, 70, 471
 Kriz, T. A., 27
 Kričevskiĭ, R. E., 32, 69, 471
 Kullback, S., 14, 15, 44, 471
 Kuznetsov, A. V., 236, 471
- Ledoux, M., 80, 471
 Leibler, R. A., 14, 471
 Leon-Garcia, A., 131, 466
 Leung, C. S. K., 300, 464
 Levin, L., 456, 469
 Li, Q., 285, 475
 Li, S-Y R., 462, 475
 Li, W., 464
 Liang, Y., 298, 460, 471
 Liao, H. J., 302, 471
 Lind, D., 70, 471
 Linder, T., 140, 471
 Littlewood, J. E., 44, 469
 Ljubic, Yu L., 66, 471
 Longo, G., x, 27, 32, 33, 168, 465, 472
 Lovász, L., 101, 102, 208, 265, 465, 472

- Lubell, L., 204, 472
 Luby, M., 456, 469
 Lugosi, G., 140, 471
 Lukács, E., x
 Lynch, T. J., 70, 472
- McLeod, J. B., 13, 464
 Malvenuto, C., 207, 470
 Marcus, B., 70, 471
 Marcus, R. S., 70, 471, 474
 Margulis, G. A., 80, 472
 Marton, K., x, 32, 80, 100, 105, 139, 142, 143, 166,
 176, 183, 266, 267, 268, 345, 353, 371, 372,
 374, 381, 382, 383, 384, 388, 389, 390, 399,
 465, 470, 471, 472
 Massey, J. L., 27, 472
 Matúš, F., 47, 459, 472
 Maurer, U. M., 450, 452, 458, 459, 463,
 472
 McEliece, R. J., 80, 141, 175, 466, 472
 McGregor, A., 174, 463
 McMillan, B., 59, 70, 472
 Meshalkin, L. D., 204, 472
 Meulen *see* Van der Meulen, E. C.
 Moore, E. F., 62, 469
 Moroga, S., 129, 472
- Nagaoka, H., 47, 463
 Nakiboğlu, B., 463
 Narayan, P., xi, 179, 228, 233, 454, 455, 458, 459,
 460, 464, 465, 466
 Nayak, I. J., 207, 208, 472
 Nemetz, T., 61, 470, 472
 Neuhoff, D. L., 139, 472
 Ng, C. T., 13, 461, 472
 Nisan, N., 455, 473
 Nitinawarat, S., xi
- Omura, J. K., 139, 165, 173, 175, 472, 473
 Oohama, Y., 267, 473
 Ornstein, D. S., 65, 473
- Pasco, R., 68, 473
 Patterson, G. W., 59, 474
 Perles, M., 79
 Pilc, R., 140, 473
 Pilotto, C., 205, 471
 Pinsker, M. S., 44, 179, 233, 236, 383, 396, 464,
 468, 473
 Pippenger, N., 46
 Plotkin, M., 80, 170, 473
 Poljak, S., 208, 473
 Poltyrev, G. Š., 377, 379, 473
 Pólya, G., 44, 469
 Poor, V., 460, 471
 Posner, E. C., 141, 472
 Prelov, V. V., 399, 468
- Pultr, A., 208, 473
 Pursley, M. B., 466
- Rackoff, C., 456
 Rajscki, C., 43, 473
 Renner, R., 446, 453, 473
 Rényi, A., v, xi, 13, 15, 31, 207, 208, 473
 Reza, F. M., 47, 473
 Richardson, T., 106, 473
 Rimoldi, B., 463
 Rissanen, J., 15, 68, 474
 Robert, J.-M., 456, 459, 463
 Rodemich, E. R., 472
 Rödl, V., 208, 467, 473
 Rose, K., 207, 208, 472
 Rumsey, H., 472
 Ryabko, B., 131, 468, 474
- Sali, A., 206, 474
 Sanov, I. N., 29, 474
 Sántha, M., 456, 474
 Sardinas, A. A., 59, 474
 Sauer, N., 79, 474
 Schmetterer, L., 14, 474
 Schneider, K., 63, 470
 Schrijver, A., 440, 474
 Schützenberger, M. P., 13, 60, 70, 474
 Seress, A., 467
 Ševerdjaev, A. Ju. *see* Ševerdyayev, A. Ju.
 Ševerdyayev, A. Ju., 165, 179, 473
 Sgarro, A., x, 33, 388, 472, 474
 Shamai, S., 460, 471
 Shannon, C. E., ix, xv, xvi, xix, 13, 14, 32, 47, 59,
 65, 66, 70, 70, 95, 97, 99, 101, 103, 104,
 105, 117, 119, 131, 143, 161, 168, 169, 172,
 175, 177, 183, 203, 235, 292, 301, 302, 445,
 458, 474
 Shelah, S., 79, 474
 Shepp, L., 464
 Shields, P. C., 15, 466
 Shor, P. W., 59, 475
 Shtarkov, Y., 70, 476
 Simon, J., 61, 472
 Simonovits, M., xi, 207, 463
 Simonyi, G., xi, 143, 205, 206, 207, 208, 265, 464,
 465, 468, 471, 474, 475
 Sinai, J. G., 65, 475
 Sinaimeri, B., 207, 471
 Slepian, D., 271, 295, 302, 475
 Smorodinsky, M., 65, 475
 Sobel, M., 62, 475
 Somekh-Baruch, A., 471
 Sperner, E., 208, 475
 Stambler, S. Z., 231, 239, 466, 475
 Stein, C., 14
 Stiglitz, I. G., 239, 475
 Strassen, V., 15, 102, 475

- Surányi, J., 102, 469
 Szekeres, Gy., 143, 475
- Talagrand, M., 80, 475
 Telatar, E., 463
 Thitimajshima, P., 106, 463
 Thomas, J. A., xi, 59, 464, 465
 Thomasian, A. J., 106, 183, 225, 227, 231, 235, 238, 239, 463, 475
 Tjalkens, J., 70, 476
 Topsøe, F., 44, 129, 467, 475
 Tóth, A., 464
 Trevisan, L., 459, 475
 Trofimov, V. K., 32, 471
 Tsybakov, B. S., 119, 236, 466, 471
 Tunstall, B. P., 63, 475
 Turán, P., 143, 475
 Tusnády, G., x, 64, 67, 70, 465
 Tuza, Z., 143, 208, 471, 473
 Tyagi, H., xi
- Ulrey, M. L., 294, 475
 Urbanke, R., 106, 285, 473, 475
- Vaccaro, U., 206, 208, 468
 Vadhan, S. P., 459, 475
 Van der Meulen, E. C., 300, 371, 381, 399, 463, 475, 476
 Vapnik, V. N., 79, 475
 Várnai, É., x
 Vazirani, U., 456, 474
- Vembu, S., 446, 475
 Verdú, S., 106, 130, 446, 471, 475
- Wallace, M. S., 466
 Wallmeier, H. M., 288, 463
 Wegman, M. N., 11, 464
 Wei, V. K., 140, 476
 Weiss, L., 102, 476
 Welch, L. R., 472
 Willems, F., 70, 300, 460, 476
 Witsenhausen, H. S., 265, 344, 346, 476
 Wolf, J. K., 271, 295, 300, 302, 460, 468, 475, 476
 Wolf, S., 446, 450, 452, 453, 458, 459, 472, 473
 Wolfowitz, J. K., 32, 96, 105, 119, 163, 165, 183, 225, 226, 236, 238, 239, 297, 462, 470, 476
 Wyner, A. D., 11, 343, 348, 352, 353, 374, 375, 376, 392, 394–395, 399, 459, 460, 469, 476
- Xin, Y., 298, 470
- Yamamoto, K., 182, 204, 476
 Yang, E., 140, 477
 Yeung, R. W., 46, 47, 462, 470, 476, 477
- Zeger, K., 140, 471
 Zhang, Z., 43, 46, 140, 476–477
 Zigangirov, K. Sh., 180, 181, 477
 Ziv, J., 343, 352, 374, 376, 399, 476
 Zuckerman, D., 455, 456, 458, 469, 473, 477

Index of symbols and abbreviations

For the basic notation and symbols used throughout the book see pp. xii–xiii. This list includes notation introduced in the text and used repeatedly without reference. The page numbers in the right-hand column show the number of the page where first used.

ABC	asymmetric broadcast channel 354
AEP	asymptotic equipartition property 58
AVC	arbitrarily varying channel 209
A*VC	224
AVS	arbitrarily varying source 135
BC	broadcast channel 354
BCC	broadcast channel with confidential messages 414
BSC	binary symmetric channel 97
(c, Γ)	input constraint 91
$c(P)$	91
C, C_ε	capacity, ε -capacity 84
C_0	zero-error capacity 84, 95
$C_{0,f}$	zero-error capacity with feedback 104
$C(\mathbf{A}, \varepsilon) = C_W(\mathbf{A}, \varepsilon)$	ε -capacity of a set 89
$C(\Gamma)$	capacity-constraint function 91, 120
$C(G)$	capacity of graph G 186
$C(G, P)$	graph capacity within distribution P 186
$C(\mathcal{G})$	Sperner capacity of digraph family \mathcal{G} 196
$C(\mathcal{G}, P)$	Sperner capacity within distribution P 196
$C = C(W)$	capacity of DMC $\{W\}$ 88
$C(\mathcal{W})$	175
$C_a = C_a(\mathcal{W})$	a-capacity of AVC $\{\mathcal{W}\}$ 210
$C_m = C_m(\mathcal{W})$	m-capacity of AVC $\{\mathcal{W}\}$ 210
C_S	secrecy capacity 411
C_{SK}	secret key capacity 424
$C_{PK}(\mathbf{A}), C_{PK}(\mathbf{A} \mathbf{D})$	private key capacity 436
$\mathcal{C}(\mathbf{M} \rightarrow \mathbf{X}, \mathbf{Y} \rightarrow \mathbf{M}')$	family of codes 214
CR	common randomness 421
CSI	channel state information 104
$\chi(G)$	chromatic number of graph G 101
d.e.s.	doubly exponentially surely 404
d_H	Hamming distance 40
$d(G), d_G(x)$	degree of hypergraph G or its vertex x 189
$d(\mathbf{x}, \mathbf{y}) = \frac{1}{k} \sum d(x_i, y_i)$	averaging distortion measure 108
$(d, \Delta), (\mathbf{d}, \Delta)$	fidelity criterion 107, 252
$d(P, W)$	108

- d_W
 D_c
 $D(P||Q)$
 $D(V||W|P)$
 DM
 DMC
 DMS
 DMMS
 $e(W, f, \varphi)$
 $\bar{e}(W, f, \varphi)$
 $e_m(W, f, \varphi)$
 $e(\mathcal{W}, f, \varphi)$
 $\bar{e}(\mathcal{W}, f, \varphi)$
 $E(G), \mathcal{E}(G)$

 $E(R) = E(R, W)$
 $E_r(R) = E_r(R, W)$
 $E_r(R, P) = E_r(R, P, W)$
 $E_{sp}(R) = E_{sp}(R, W)$
 $E_{sp}(R, P) = E_{sp}(R, P, W)$
 $E_x(R) = E_x(R, W)$
 $E_x(R, P) = E_x(R, P, W)$
 $\mathcal{F}(X; Y, Z|X)$
 $g_W(\mathbf{A}, \eta)$
 $G(W)$
 $\mathcal{G}(G)$
 $\mathcal{G}(X; Y; Z|X)$
 $\mathcal{G}(Y; Z|X)$
 $\mathcal{G}^*(X; Y; Z|X)$
 $\Gamma \mathbf{B}, \Gamma^l \mathbf{B}$
 $H(G, P)$
 $H(P), H(X)$
 $H(\mathbf{x})$
 $H_\alpha(P)$
 $H_\infty(P)$
 $\bar{H}(X^\infty)$
 $H(Y|X), H(W|P)$
 $\mathcal{H}(X; Y; Z|X)$
 $\mathcal{H}_k(X; Y; Z|X)$
 $\mathcal{H}^*(X; Y; Z|X)$
 $\mathcal{H}^*(Y; Z|X)$
 $I(X \wedge Y), I(P, W)$
 $I(\mathbf{x} \wedge \mathbf{y})$
 $I(X \wedge Y|Z)$
 $I(P, \mathcal{W})$
 $l(\mathbf{x})$
 $\bar{l}(f)$
 LMTR
 $\Lambda(\mathbf{A}), \Lambda(\mathbf{A}|D)$
 $\mathbf{M} = \mathbf{M}_f$
 MA
 MAC
 MMI
 $[n]$
 $N(a|\mathbf{x}), N(a, b|\mathbf{x}, \mathbf{y})$
 NSN
 OS

 distortion measure associated with channel W 165
 set of inputs to be reproduced at c 252, 280
 informational divergence 7
 conditional divergence 18
 discrete memoryless
 discrete memoryless channel 84
 discrete memoryless source 3
 discrete memoryless multiple source 246
 maximum probability of error 83
 average probability of error 83
 probability of erroneous transmission of message m 83
 maximum probability of error, family of channels 154
 average probability of error, family of channels 154
 set of edges (hyperedges) of graph (hypergraph) G 185, 189
 reliability function 152
 random coding exponent 152
 random coding exponent, constant composition codes 147
 sphere packing exponent 152
 sphere packing exponent, constant composition codes 149
 expurgated exponent 165
 expurgated exponent, constant composition codes 165
 region of achievable entropy triples 305
 image size 85
 graph associated with channel W 101
 digraph family generated by graph G 201
 region of achievable exponent triples 305
 projection of $\mathcal{G}(X; Y; Z|X)$ 317
 323
 Hamming neighborhood, l -neighborhood 71
 graph entropy 141
 entropy 3, 4
 entropy of individual sequence 35
 Rényi entropy of order α 13
 minentropy 13
 entropy rate 51
 conditional entropy 8, 18
 304
 304
 313
 317
 mutual information 8, 34
 mutual information of individual sequences 35
 conditional mutual information 35
 154
 length of a sequence 49
 average codeword length 49
 limit of minimum transmission ratio xix
 440
 message set 83
 multiple-access 272
 multiple-access channel 272
 maximum mutual information 100, 147
 the set $\{1, \dots, n\}$ 193
 16, 17
 normal source network 254
 omniscience 436

484 **Index of symbols and abbreviations**

$\omega(G), \omega_s(D)$	size of largest clique or symmetric clique of graph G or digraph D 101, 185, 194
$P_{\mathbf{x}}, P_{\mathbf{x},\mathbf{y}}$	type, joint type of sequences 16, 17
PK	private key 426
$r(f, X^k), r(k)$	redundancy, minimax redundancy 67, 68
R_{cr}	critical rate 152
R_{cr}^*	173
$R(\Delta), R_\varepsilon(\Delta)$	108
$R(\Delta) = R(P, \Delta)$	rate-distortion function 108, 120
$R_{\text{OS}}(\mathbf{A}), R_{\text{OS}}(\mathbf{A} \mathbf{D})$	smallest achievable OS rate 436
$\mathcal{R}(X, Y, Z)$	achievable rate region of fork network 247
$\mathcal{R}((X), Y)$	361
$s(P)$	support size of P 24
\mathbf{S}_b	250
$\mathbf{S}_W(x)$	support of the distribution $W(\cdot x)$ 184
$S(K Z)$	security index 400
SK	secret key 421
SMD	standard minimum distance 211
$T_P = T_P^k$	set of sequences of type P 16
$T_{[P]_\delta} = T_{[P]_\delta}^k, T_{[X]_\delta} = T_{[X]_\delta}^k$	set of typical sequences with given δ 20
$T_{[P]} = T_{[P]}^k, T_{[X]} = T_{[X]}^k$	set of typical sequences with $\delta = \delta_k$, cf. Delta-Convention 21
$T_V(\mathbf{x}) = T_V^k(\mathbf{x})$	V -shell 18
$T_{[W]_\delta}(\mathbf{x}) = T_{[W]_\delta}^k(\mathbf{x})$	} set of generated sequences with given δ 20
$T_{[Y X]_\delta}(\mathbf{x}) = T_{[Y X]_\delta}^k(\mathbf{x})$	
$T_{[W]}(\mathbf{x}), T_{[Y X]}(\mathbf{x})$	set of generated sequences with $\delta = \delta_k$, cf. Delta-Convention 21
$T_{[W]}(\mathbf{A}) \triangleq \bigcup_{\mathbf{x} \in \mathbf{A}} T_{[W]}(\mathbf{x})$	306
$\tau(G), \tau^*(G)$	edge covering resp. fractional edge covering number of hypergraph G 189
$V(G)$	vertex set of (hyper)graph G 185, 189
$\{W\} = \{W : X \rightarrow Y\}$	discrete memoryless channel 84
$\{\mathcal{W}\} = \{\mathcal{W} : X \rightarrow Y\}$	arbitrarily varying channel 209
$X_{\mathbf{A}}$	vector of RVs $X_a, a \in \mathbf{A}$ 246
$\mathbf{X}_{\mathbf{A}}$	Cartesian product of sets $X_a, a \in \mathbf{A}$ 251

Subject index

- ABC coding theorem 360
 alternative form, 371
 converse part, 359–360
 direct part, 354–357
 with input constraint, 383
 see also asymmetric broadcast channel
- a-capacity, AVC, 210, 214–224, 239
 coding theorem, 218–220
 positivity, 227–228
- a-capacity and m-capacity
 difference, for AVC, 229
 equality
 DMC, 93
 AVC with stochastic encoder, 220–222
- a-capacity region *see* capacity region
- a-capacity region and m-capacity region
 difference, MAC, 285
 equality
 broadcast channels, 293
 stochastic encoders, 286, 292–293
- achievable entropy triples, 304
 see also entropy characterization problem
- achievable exponent triples, 304, 305
 see also image size characterization problem
- achievable (ϵ -achievable) rate
 channel 84–85
 source, at distortion level Δ , 107
 wiretap channel, 410–411
 see also common randomness; omniscience;
 private key; secret key
- achievable (ϵ -achievable) rate-distortion pair, 108
- achievable (ϵ -achievable) rate pairs
 ABC coding theorem, 360
 for multi-access channels, 273–274, 279, 288
- achievable (ϵ -achievable) rate region
 channel network *see* capacity region
 fork network *see* fork network
 optimal points of region, 247
 source network, 252, 257–258, 264
 product space characterization, 262
 see also source network coding theorems
- achievable (ϵ -achievable) rate triple, fork network,
 246–247
- achievable (ϵ -achievable) rate vector
 channel network, 282
 source network, 252, 253
- active feedback, 229
- additive noise, 98
- additivity of information measures, 12, 36, 37
- addressing, 280
- algebraic codes *see* linear code
- alphabet
 channel input and output, xvii, 84, 272
 code, 48
 reproduction, 107
 source, 3
- alphabetic prefix code, 62
- amount of information, xv, xix, xx, 7
 unit of, xx
 see also information measures
- antiblocker, 142
- arbitrarily “star” varying channel (A^*VC), 224, 235
- arbitrarily varying channel (AVC), 209 ff.
 capacity
 a- and m-capacity, 210
 positivity, 225, 227–228
 for random codes, 217, 226–227
 with stochastic encoder, 220
- coding theorems
 a-capacity, 220
 m-capacity, binary output, 213
 stochastic encoder, 220
- feedback, 229, 234–235
- game-theoretic approach, 222–223, 230–231
- source-channel transmission, 229–230
- states depending on inputs, 224, 235–236
- states known at input or output, 223–224,
 231–233, 235–236
- stochastic decoder, 230
- and zero-error capacity of DMC, 225–226
- arbitrarily varying multi-access channel (AVMAC),
 290–291
- arbitrarily varying source (AVS), 135, 140, 222
- arithmetic code, 68, 69
- asymmetric broadcast channel (ABC), 354 ff
 a- and m-capacity regions equal, 357

- coding theorem *see* ABC coding theorem
- with confidential messages *see* broadcast channel
 - with confidential messages (BCC)
- asymptotic equipartition property (AEP), 58–59
- asymptotics, refined
 - in Noisy channel coding theorem, 102
 - of average distortion, 140
 - of error probability, sources, 32
 - of minimax redundancy, 69
 - of high probability set size, 11
 - of size of T_p^k , 26
- attainable error exponent
 - see* error exponent
- automata, as noiseless channels, 66
- average codeword length, 70
- Average cost theorem, 52–54, 56
 - alternative proof of converse, 59, 62
- average fidelity criterion, 107, 113
- Average length theorem, 49
 - see also* Average cost theorem
- average probability of error, 83, 154
 - capacity for *see* a-capacity
 - family of channels, 154
 - at output c , channel network, 282
- averaging distortion measure, 108
- axiomatic approach, 9, 12–13

- belief propagation algorithm, 94, 106
- better in the Shannon sense (channel), 99
- binary adder, 388–392
- binary block code, 3
 - expected common length, 393
- binary channel, 211
 - images for, 343–344
 - noiseless, xix
 - symmetric *see* binary symmetric channel
- binary erasure channel (BEC), 97
- binary entropy function, xiii
- binary symmetric channel (BSC), 97
 - capacity, 97
 - error bounds, 174–175
 - with feedback, 180–181
 - images over, 342–343
 - linear codes, 97, 179
- binning, random, 257, 263
- bit, xix
- block code, xix
 - (n, ε) -code, 84, 89, 92–3
 - channel networks, 280
 - channels, 84
 - feedback, 103
 - multiple-access (MA), 273
 - stochastic encoder and decoder, 220, 230
 - fork network, 246
 - k -to- n , 113
 - binary, 3
 - source-channel networks, 283
 - source networks, 252
 - sources, 3, 107
 - with side information at the decoder, 243
 - see also* linear code
- blockwise coding, xix
- Blowing up lemma, 76–78, 80, 89, 339, 392
- Bollobás pairs, 205–206
- Borel–Cantelli lemma, 60
- branching property, 12
- broadcast channel (BC), 293, 354
 - a- and m-capacity are equal, 293
 - asymmetric two-output *see* asymmetric broadcast channel (ABC)
 - bounds on capacity region, 372, 381
 - with comparable components 374
 - with confidential messages (BCC), 414–421, 459
 - degraded, 372–374
 - product of, 377–379
 - sum of, 379–381
 - with degraded message sets *see* asymmetric broadcast channel
 - deterministic, 382–383
 - zero-error, 383
 - semi-deterministic, 383
 - see also* ABC coding theorem; asymmetric broadcast channel
- capacity (ε -capacity), xix, 84
 - alternative definitions, 93
 - alternative formulas, DMC, 88, 124, 128–129
 - as information radius, 124, 128–129
 - computation *see* computation of, capacity of a DMC
 - explicit formulas, 97
 - with feedback *see* feedback
 - generalized (for given order of magnitude of error probability), 159, 164
 - independence of ε *see* strong converse
 - under input constraint, 91, 95, 100, 124
 - under output constraint, 100
 - region *see* capacity region
 - secrecy, 444, 459
 - wiretap channels, 411–414
 - set capacity, 89
 - asymptotic independence of ε , 90
 - unit cost, DMC, 103, 130
 - zero-error *see* zero-error capacity
 - see also* arbitrarily varying channel; compound DMC; noiseless channel
- capacity computing algorithm, 123–124, 131
- capacity-constraint function, 120, 129
 - alternative formula, 124
 - concavity, 92
 - differentiability, 129
 - distribution achieving, 129
- capacity of graphs
 - see* graph, capacity; Sperner capacity

- capacity, private key, 427, 436, 444
 and multi-information, 455
 multi-terminal channel model, 441
 multi-terminal source model, 438–440
- capacity, secret key, 423–426, 444, 459
 definition equivalence, 449–451
 multi-terminal, 458, 460
 for one-way source model, 427–435
 upper bounds of, 452–453
- capacity region (ϵ -capacity region), 274, 282
 a- and m-regions *see* a-capacity region and m-capacity region
 alternative definitions, 284, 302 283, 301
 characterization
 computable *see* broadcast channel;
 multiple-access channel; two-way channel
 product-space, 302
 effect of feedback, 299
 relevance for source-channel transmission, 283, 284, 288, 293
 stochastic encoders, 286, 292
- Carathéodory-Fenchel theorem, 310
- chain rules, 36
- channel, xvi–xvii
 coding theorem *see* coding theorem, for channels
 comparison of, 99–100, 344–345
 equidistant, 174
 as matrix, 83
 as matrix sequence, 106
 multiterminal *see* channel network
 product of, 98
 sum of, 98–99
 symmetric, 97, 180
see also arbitrarily varying channel; binary channel; channel network; compound channel; discrete memoryless channel; noiseless channel
- channel model of secret key generation *see* secret key, generation of
- channel network, 280–284
 capacity region *see* capacity region
 coding theorems *see* broadcast channel;
 multiple-access channel; two-way channel
 component channels, 281, 369
 of depth 2, 280–283, 303
 normal, 301
 with one intermediate vertex *see* broadcast channel
 with one output vertex, 294
 reduction of problems, 301–302
- channel noise, xvii, xviii
 additive, 98
- channel state information (CSI), 104, 223
 non-causal, 104, 223, 225, 236–237
see also arbitrarily varying channel (AVC)
- chromatic number of graph, 101–102, 265
 fractional, 207
 local, 205
- ciphertext, 445
- clique, 185, 186
 of digraph family, 194
 symmetric, 194, 195, 196–197
- clique number, 185, 189, 193
 symmetric, 194
- code, xvi, xviii
 alphabetic, 62
 arithmetic, 68, 69
 associated with a network, 251
 block *see* block code
 for channels with input set X and output set Y , 83
 composed, 59–60
 constant composition, 100, 141
 fixed-length-to-fixed-length, xix
 fixed-to-variable length, 48–61
 Gilbert–Moore, 60
 Huffman, 58
 infinite, 64
 instantaneous, 57
 for k -length messages, 83
 linear *see* linear code
 list, 175–176
 low density parity check (LDPC), 94, 106
 multiple-access (MA), 281–282
 (n, ϵ) code, 84, 89, 92–93
 prefix *see* prefix code
 random, 214
 redundancy, 67
 Shannon–Fano, 70
 separable, 48
 sliding block, 64
 suffix, 60
 synchronizing, 60
 Tunstall, 63
 turbo, 94, 106
 universally optimal *see* universally optimal code
 variable length *see* variable length code
 with feedback, 103
 with stochastic encoder, 220, 286–287, 292–293
- code alphabet, 48
 code selector, 222
 code tree, 49
 saturated, 58
see also tree representation
- coder (of a network), 251
- code-stuffed sets, 328, 341
- Code stuffing lemma, 331–335
- codeword, xviii–xix, 48, 83
 length, and information of an event, 60–61
- coding theorem (definition), 93
 converse part *see* converse result
 direct part *see* direct result

- for channels *see* arbitrarily varying channel; compound DMC; discrete memoryless channel
- for channel networks *see* broadcast channel; multiple-access channel; two-way channel
- for source-channel transmission *see* source-channel, transmission theorem
- for sources *see* source coding theorems
- for source networks *see* source network coding theorems
- noiseless *see* Average cost theorem; Average length theorem
- Noisy channel coding theorem, 88–89
- practical significance, 88–89
- remainder terms, *see* asymptotics, refined *see also* exponential probability bounds
- coloring, 101, 205
 - fractional, 207
- combinatorial lemmas, 16 ff., 71 ff.
 - packing, 145–147
 - type covering, 132–134
- common information, 393–395
 - latent, 452
- common length (of binary block codes), 393
- common randomness (CR), 421, 443, 459
 - capacity, 423–424
 - secret *see* private key; secret key
- communication model (varying-state channel), 222–223
 - capacity, 223
- communication protocols for generating CR
 - ε -omniscience, 436
 - for channel model, 422–423
 - non-interactive, 435, 436, 437, 438, 442, 458
 - for source model, 422, 423
 - multi-terminal, 435, 436, 437, 438
- communication system, Shannon’s model of, xv ff.
- comparable component channels, 369
- comparison of channels, 99–100, 344–345
- component channel (of a channel network), 281
- component source (of a DMMS), 246
- composed code, 59–60
- composite source *see* compound source
- composition class *see* type class
- compound channel, 154
 - coding theorem, 155–159, 163, 187
 - discrete memoryless *see* compound DMC
 - multiple-access, 289–290
- compound DMC, 154
 - coding theorem 155
 - invalidity of strong converse, 163
 - maximal codes for, 163
 - reliability function, 154
 - zero error capacity, 186–189, 193
 - with informed decoder, 163, 187, 206, 265, 289
- compound source, 139, 140
 - computable characterization, 261–263
 - computation of
 - capacity of a DMC, 123–124
 - Muroga’s method, 129
 - simple channels, 97
 - capacity-constraint function, 123
 - Δ -distortion rate, 126–128, 128
 - error exponent
 - in channel coding, 171–172
 - in hypothesis testing, 30–31
 - in source coding, 30–31
 - rate-distortion function, 126, 129–130
 - conclusive result, 369
 - conditional
 - distribution, xiii
 - entropy, 7–8, 14, 18, 35
 - informational divergence, 18
 - Markov chain, 40
 - mutual information, 35, 416
 - type, 18
 - connected by channel W (RVs), 83
 - conservation of entropy, 63–65, 67
 - and ergodic theory, 64–65
 - constant composition codes, 100, 144 ff.
 - expurgated bound, 166
 - Gilbert bound, general, 160
 - random coding bound, 147–148
 - universal attainability of, 154
 - universal improvement of, 163
 - reliability at zero rate, 168–169
 - sphere packing bound, 148–150
 - undetected error and erasure, 156
- constraint upon the codewords, 91
 - see also* input constraint
- context tree weighting data compression
 - algorithm, 70
- continuity lemmas
 - entropy, 19, 43
 - metric, 42–43
 - Fano’s inequality, 39–40
 - random coding exponent function, 151
 - rate-distortion function, 108
- converse results, 93
 - see also* exponential probability bounds; strong converse; weak converse
- convex closure, xiii, 210
 - of stochastic matrices set, 210
 - row-convex closure, 210
- convex corner, 141–142, 143
 - antiblocker, 142
 - entropy relative to, 141–142
- convexity
 - of achievable rate regions and capacity regions
 - see* time sharing principle
 - of capacity-constraint function, 92
 - of expurgated exponent function, 167

Subject index

489

- of function of distributions or channels, xiv
 - of information measures, 37
 - lemma, 37
 - of rate-distortion function, 108–109
 - of sphere packing exponent function, 150
 - Core theorem, 195–198, 203, 207
 - correlated random code *see* random code
 - correlated source *see* discrete memoryless multiple source
 - cost, 52, 103
 - function, general, 56
 - of transmission, xvi, xviii
 - covering
 - number, 189
 - Hypergraph covering lemma, 190
 - Type covering lemma, 132–134
 - see also* Edge cover lemma
 - Cramér–Rao inequality, 14
 - critical rate, 152, 162
 - $E_X(R) = E_{\text{Sp}}(R)$ at c.r., 173
 - for list codes, 176
 - of a BSC, 174
 - with feedback, 180
 - cross-entropy *see* informational divergence
 - crossover probability, BSC, 97
 - cyclic triangle, 204

 - data compression *see* source coding theorems
 - Data processing lemma, 63
 - strong form, 45, 345
 - data storage, xvi
 - decision feedback, 181–182
 - decoder, xvi, xviii
 - channel networks, 281, 282
 - channels, 83
 - maximum likelihood, 111
 - maximum mutual information, 100, 147–148, 164
 - minimum distance (MMI), 97
 - standard (SMD), 211
 - choice of, 160
 - informed, 163–164
 - joint typicality, 96, 100, 160, 237
 - minimum entropy, 160
 - network, 251
 - source, 107
 - stochastic, 230
 - decoding, xvi
 - maximum likelihood, 160, 171
 - MMI, 160, 183
 - decoding set, 392
 - degraded channels, 99
 - broadcast channel, 372–373
 - product of, 376–379
 - sum of, 379
 - entropy and image size characterization, 339–340
 - degree
 - of a hypergraph, 189
 - of a vertex, 189
 - delta-convention, 21, 22
 - Δ -distortion rate, 108
 - alternative definitions, 108, 112, 139
 - computing algorithm, 126–127, 131
 - discrete memoryless source, 107–112, 262
 - zero error rate, 116, 134
 - computation of, 140
 - see also* distortion measure; Rate distortion theorem
 - depth
 - of a graph, 250
 - of a vertex, 250
 - destination, xv, xvi
 - deterministic broadcast channel, 382–383
 - semi-deterministic, 383
 - digraphs, 194–196, 198, 199, 201–202, 207, 250
 - capacity *see* Sperner capacity
 - co-normal product, 194
 - power, 194
 - transitive tournament, 204
 - see also* graph; hypergraph
 - direct result, 93
 - directed graphs *see* digraphs
 - discrete memoryless broadcast channel *see* broadcast channel
 - discrete memoryless channel (DMC), 83 ff., 144 ff.
 - capacity, 120, 262
 - “MA capacity”, 285
 - coding theorem, 88, 91
 - for codewords from a given set, 90–91
 - remainder terms in, 102
 - strong converse, 93
 - weak converse, 93, 95
 - exponential probability bounds *see* error exponent, DMC
 - feedback, 103, 104
 - image of a set *see* image (of a set over a channel)
 - input constraint on *see* input constraint
 - linear codes, 97–98, 178–179
 - maximal code lemma, 85–87
 - for two channels, 316
 - multi-terminal *see* channel network
 - reliability function, 152, 153, 154
 - transmission of a source, 112 ff., 178
 - universal coding, 153–154, 156, 163
 - zero-error capacity, 104, 184
 - see also* channel
- discrete memoryless multiple-access channel *see* multiple-access channel
- discrete memoryless multiple source (DMMS), 243, 246
 - 2-source, 243
 - 3-source, 246

- coding theorems involving *see* source network coding theorems
- discrete memoryless source (DMS), 3
 - coding theorems for *see* source coding theorems
- discrimination, information for *see* informational divergence
- distance
 - distributions, variational, 19
 - and informational divergence, 44
 - random variables, entropy distance, 39, 42–43
 - sequences, Hamming *see* Hamming distance
 - see also* minimum distance
- distortion measure, xvii, 107
 - associated with a channel, 165
 - averaging, 108
 - non-finite, 117, 129–130
 - peak, 117
 - several, 117
 - single-letter, 108
- distortion-rate function, 137, 173–174
- divergence
 - contraction *see* Data processing lemma
 - geometry, 45–46
 - of order α (Rényi), 31, 32
 - projection, 45, 46
 - symmetrized, 44
 - see also* informational divergence
- double Markovity, 392–393
- doubly stochastic matrix, 43
- doubly exponentially surely, 404
- duality of source and channel problems, 263
- Duality theorem of linear programming, 440
- eavesdropper, 421–422
- edge cover (of hypergraph), 189
- Edge cover lemma, 191–192, 196, 204
- edges, of graphs, 185
- empirical distribution, 16
 - large deviation probabilities for, 29
- encoder, xvi, xvii
 - channels, 83
 - channel networks, 281, 282
 - with feedback, 103–104
 - informed, 163–164
 - networks, 251
 - separable range, 48
 - sequential, 64
 - source, 107
 - source networks, 251
 - stochastic, 220, 286–287, 292–293
 - uninformed, 199–200
- encoding, xvi
- encryption, 410, 421
- entropy, xx, 4, 9
 - achievable vectors, 349–350
 - axiomatic characterization, 9, 12–13
 - conditional, 7–8, 35
 - conservation of, 63–65, 67
 - cross-entropy *see* informational divergence
 - ε -entropy (in Russian literature) *see*
 - Δ -distortion rate
 - formal properties, 34 ff.
 - in ergodic theory, 64–65
 - of graph, 141, 142–3
 - of individual sequence, 35
 - linear equation for, 38
 - metrics for, 39, 43
 - in physics, 15, 33
 - postulational characterizations, 12–13
 - of random variable, 4
 - rate, 51, 58–59
 - relation to polynomial coefficients, 17
 - relative *see* informational divergence
 - relative to convex corner, 141, 142
 - Rényi's (order α), 13
 - structural properties, 38–39, 46–47
 - upper bounds on, 42
 - see also* entropy characterization problem
- entropy characterization problem, 263, 304 ff
 - and source networks, 263, 264, 304, 360–361
 - partial results 347 ff
 - and image size characterization problem, 338, 342
 - solution for 3-sources *see* Entropy characterization theorem
- Entropy characterization theorem, 338
- achievable triples, 305
- converse part, 313–316
- direct part, 335–338
 - see also* entropy characterization problem
- entropy function, 19–20, 46–47
 - binary, xiii
- entropy-typical sequences, 26–27
- equidistant channel, 174
- equivocation rate, 414, 415
- erasure, 155
 - binary channel (BEC), 97
 - probability of, 155
- ergodic stationary sources, 59, 60, 64–65, 446
- ergodic theory, 64–65
 - isomorphy problem, 65
- error exponent
 - compound DMC 173
 - DMC, 144 ff.
 - constant composition codes, 147–150, 171, 183
 - feedback, 179–182
 - list codes, 175
 - rates above capacity, 165
 - for two messages, 168–169
 - undetected error and erasure, 156
 - universally attainable, 153–154, 163

Subject index

491

- see also* expurgated bound; random coding bound; reliability function; sphere packing bound
- hypothesis testing, 6, 29–30
- sources, 24, 28, 30–31
 - in Rate distortion theorem, 137
- source-channel, 178
- source networks, 266, 268, 269–271
 - see also* exponential probability bounds
- error frequency fidelity criterion, 113, 116, 139
- error probability
 - for two messages, 168–169
 - see also* error exponent; probability of error
- expected common length of codes, 393
- exponential probability bounds
 - at achievable rates *see* error exponent
 - hypothesis testing, 6, 30
 - at non-achievable rates
 - channel, 164
 - source, 27, 139
- expurgated bound, 166
 - alternative formula, 171
 - BSC, 174
 - equidistant channels, 174
 - and Gilbert bound, 174–175
 - under input constraint, 171
 - product space e. b., 174
 - tightness at zero rate, 169–70
 - and zero-error capacity, 167–168
 - see also* expurgated exponent function
- expurgated exponent function, 166
 - alternative formula, 173
 - and distortion-rate functions, 173–174
 - properties of, 167–168
 - and random coding exponent function, 166, 173
- extension of a code, 85
- Extractor lemma, 402–404, 445, 446, 447, 459
- extractors, 401, 459
 - deterministic, 402, 444, 459
 - ε -extractor, 401, 447, 455–457
 - randomly selected, 445–446
 - seeded, 401, 455–457, 459
 - stochastic, 455
- extremal set theory, 193
- family of channels
 - average probability of error, 154
 - maximum probability of error, 154
 - see also* arbitrarily varying channel; compound channel
- Fano's inequality, 39–40
- feedback, 113
 - active, 182
 - for arbitrarily varying channels, 234–235
 - complete, 113, 179–181, 182, 234
 - decision, 181–182
 - and DMC capacity, 113
- error exponent, 179–182
 - multiple-access channel with, 299–300
 - passive and active, 182
 - probability of error for $R > C$, 165
 - variable-length channel codes, 104, 182
 - and zero-error capacity, 104
- Fibonacci sequence, 61
- fidelity criterion, xvi–xviii
 - average fidelity criterion (d, Δ), 107
 - for source-channel transmission, 112
 - relation to ε -fidelity criterion (d, Δ), 116, 139
 - ε -fidelity criterion (d, Δ), 107, 116, 139
 - and arbitrarily varying source, 135
 - source networks, 252–253
- error frequency, 50, 115
 - probability of error, xvii, 3, 115
 - source networks, 252
- several distortion measures, 117–118
- zero-error, 116
 - see also* distortion measure
- finite state noiseless channel, 66–67
- Fisher's information, 13–14
- Fittingof weight *see* entropy of an individual sequence
- fixed-length-to-fixed-length code, xviii
- fixed-to-variable length code, 48
- fork network, 246
 - achievable rate region 247
 - exponential error bounds, 266, 268, 269–271
 - with side information, 395–396
 - universal coding, 266
 - zero-error rate region, 265
- Fork network coding theorem, 248–50, 263, 271
- fractional chromatic number, 207
- fractional coloring, 207
- fractional edge cover, hypergraph, 189
- fractional edge covering number, hypergraph, 189
- fractional independence number, 190
- fractional independent set, 189–190
- fractional vertex packing polytope, 143
- Galois field, 11
- game-theoretic approach, 222–224, 230–231
 - see also* channel state information
- general channels, 94, 106
 - noiseless, 65–66
- generated sequence, 20
- generic distribution, 3
- generic variables, 243, 246
- Gilbert bound, 80
 - and expurgated bound, 174–175
 - general, 160
- graph, 185
 - associated with a channel, 101
 - capacity, 186, 194
 - within fixed distribution, 186
 - robust, 206, 207

- see also* Sperner capacity
 - coloring, 101, 204, 207
 - cyclic triangle, 204
 - depth of, 250
 - directed 194 ff, 250
 - see also* digraph
 - entropy, 141, 142–143
 - perfect, 102
 - product, 101
 - chromatic number and zero-error rate region, 265
 - representation
 - of codes *see* tree representation
 - of source and channel network problems *see* channel network; source network
 - and stochastic matrix, 101
 - undirected, 194, 195
 - group code *see* binary symmetric channel, linear code
- Hamming
- boundary, 71, 74
 - distance, 40
 - and conditional entropy, 40
 - and mutual information, 100
 - metric, 71
 - neighborhood, 71
 - probability bound on, 76
 - space, isoperimetric problem in, 78
 - sphere, 78
- Hartley's information measure, 15
- hash functions, universal family of, 456–457
- hashing, perfect, 176
- helpers, 255, 263, 268–269, 370
 - in arbitrary source network, 269
 - two, 388–390
- Helpers theorem, 258–261, 264, 360
- high probability sets
 - minimum cardinality of, 3
 - minimum mass of, 5, 6
- Hoeffding's inequality, 21, 44
- Huffman code, 58
 - word length and probability in, 60
- hypergraph, 189–192
 - degree of, 189
 - edge cover, 189
 - fractional edge cover, 189
 - fractional edge covering number, 189
 - r -uniform, 189
 - rank of, 189
 - regular, 189, 191–192
- Hypergraph covering lemma, 190–191, 207
- hypothesis testing, 6–7, 9–10, 11–12, 29–30, 59
- I-divergence *see* informational divergence
- identification capacity, 459
- image (of a set over a channel), 85
 - η -images, 85, 305, 339
 - and generated sequences, 346–347
 - quasi images, 346–350
 - see also* image size (η -image size)
- image size (η -image size), 85
 - asymptotic independence of η , 89
 - binary channels, 339, 343–344
 - and ε -capacity of a set, 89
 - and information quantities, 307
- image size characterization problem, 304 ff
 - achievable exponent triples, 305
 - relation to entropy characterization problem, 324, 338, 342
- three channels, 352
- unrestricted, 341
- Image size theorem, 328
 - converse part, 325
 - direct part, 326
 - projections in, 328
 - degraded case, 322, 339–40
- inaccuracy, 19
- indecomposable joint distribution, 345
- independent set, 189–191
 - fractional, 189–190, 191
- independent sources, transmission of, 288, 293
- induced subgraphs, 102, 185, 194
- infinite code, 64
- information, xv
 - amount of, xix, 4, 7, 9
 - common, 393–395
 - content in an RV, xx, 4
 - for discrimination *see* informational divergence
 - gain *see* informational divergence
 - geometry, 47 *see also* divergence geometry
 - inequality, 46
 - non-Shannon-type 46
 - measures of *see* information measures
 - metrics *see* entropy, metrics
 - mutual *see* mutual information
 - provided by an event, 20
 - and codeword length, 60–61
 - radius, 128–129
 - pseudo-, 13
 - source *see* source
 - storage, xv, xix
 - transmission theorem *see* source-channel, transmission theorem
- information measures, xv, xix, xx, 9, 34 ff
 - additivity of, 36
 - and additive set functions, 38–39
 - axiomatic and pragmatic approaches, 9
 - convexity of, 37
 - intuitive concept of, xv–xvi
 - Fisher's, 13–4
 - Hartley's, 15
 - individual sequences, 35

- Kullback's *see* informational divergence
 non-negativity, 36
 Rényi's *see* entropy
 Shannon's, 15, 34 ff
see also common information; entropy;
 informational divergence; mutual
 information
- informational divergence, 7
 and variational distance, 44
 conditional, 18
 convexity of, 37
 decrease of, in indirect observation *see* data
 processing lemma
 geometry of *see* divergence geometry
- input alphabet, xvii, 84, 272
 input constraint (c, Γ), 91
 average, 95, 163
 capacity under, 91
 reliability function under, 163, 171
 multiple, 100
- input of a network 250–251
 input set, 83
 input vertex, 250
- instantaneous code, 57
- interference channel, 296–298
 cognitive, 298, 444, 460
 with common messages, 298
- intermediate vertex, 250
- interval graph 118
- intrinsic randomness, 446
- intuitive background, xv–xviii
 measuring information, xx
 multi-terminal systems, xx–xxi
- isomorphy problem in ergodic
 theory 65
- isomorphic sources, 64
- isoperimetric problem, 71, 78
- joint type, 17
- joint ξ -typicality, 407–408
- jointly typical sequence pairs, 20
- juxtaposition of codes, 247
 MA codes, 274
- Key identity lemma, 413, 414, 415, 416,
 428, 443, 459
- Kolmogorov probability space, xv
- Kolmogorov–Sinai theorem, 65
- Kraft inequality, 58–59
 generalized, 55, 59
- Kullback–Leibler information number *see*
 informational divergence
- large deviation probabilities for empirical
 distributions, 29
- Leftover hash lemma, 456–457
- less noisy (channels), 344, 411, 452
- limit of minimum transmission ratio (LMTR), xviii,
 9, 116
 AVS-AVC, 229
 DMS-DMC *see* source-channel, transmission
 theorem
 and information measures, xix
 multiple-access channel, 272, 285, 288
 source-channel network, 283, 293
- linear code
 for channels, 97–98, 178–179
 for sources, 33
 for source networks, 268
 binary adder source network, 389
 shifted, 98
- linear information inequality, 46
- list code, 175–176
 AVC capacity, 233
 error exponent 196
 zero error capacity, 175
- local chromatic number, 205
- log-sum inequality, 35
- low density parity check (LDPC) codes, 94, 106
- LYM inequality, 203–204
- m-capacity, AVC, 210
 and zero-error capacity of a DMC, 225–226
 positivity, 225
see also a-capacity and m-capacity
- m-capacity region *see* capacity region
- MA capacity, 285
- MA code, 272
 block, 273
 with stochastic encoders, 286–287
- Markov chain, xiv, 40–41
 double Markovity, 392–393
- max-closure, 340–341
- maxentropy, 13
- Maximal code lemma, 85–87
 for compound channels, 163
 converse, 87
 for two channels, 316
- maximum likelihood decoder, 94
 and minimum distance decoder, 97, 212
- maximum mutual information (MMI) decoder,
 100, 147
 modified, 157
- maximum probability of error, 83, 154
 capacity for *see* m-capacity
 capacity region for *see* m-capacity region
 for family of channels, 153
 at output c , channel network, 282
- Mealy automaton, 66
- measure concentration, 80
- message, xvi, xvii, 83
 addressing of, 280
 of length k , xvii
 random, xvii

- set, 83, 272, 281
- vector, 282
- metrics, 39–40, 43
- minentropy, 13, 404, 446
- minimax redundancy, 68, 130–131
 - asymptotics, 69
- minimax strategy, 231
- Minimax theorem, 129, 211, 231, 442
- minimum distance
 - decoder, 97, 228
 - standard (SMD) decoder, 211, 212–213
 - Gilbert bound, 80
 - JPL bound, 80
 - Plotkin bound, 80
- minimum entropy decoder, 267
- Moore automaton, 66
- more capable (channel), 99, 344
- more uniform distribution, 12, 44
- multiple-access channel (MAC), 272
 - adder, 273
 - arbitrarily varying (AVMAC), 290–291
 - capacity region (a-capacity region), 272
 - alternative definition, 274, 279
 - and m-capacity region, 285
 - coding theorem, 277–279
 - alternative form, 279
 - compound, 289–90, 294
 - with common messages, 294
 - with feedback, 299–300
 - generalized *see* channel network, with one output vertex
 - LMTR for, 272, 284, 288
 - with s senders and r receivers, 293
 - stochastic encoders, 286–287
 - two-input two-output, 289
 - zero error code, 285
- multiple-access code *see* MA code
- multiple source *see* discrete memoryless multiple source
- multi-information, 43, 455
 - and PK capacity, 455
- multi-terminal coding theorems *see* channel (source) network, coding theorems
- multi-terminal systems
 - see* channel network; source-channel network; source network
- mutual information, 8
 - and common information, 395
 - conditional, 35
 - convexity, 38
 - maximum mutual information decoder (MMI), 100, 147
 - of individual sequences, 35
 - of several RVs, 43
- mutual quasi-images, 346
- n -length block code *see* block code
- network, 250–251
 - associated code, 250–251
 - alternative definition, 271
 - coders, 251
 - see also* channel network; source-channel network; source network
- Neyman–Pearson lemma, 9–10
- noiseless channel, xvii, xix, 53, 65–67
 - capacity per unit cost, 53
 - definition by source-channel transmission, 53
 - direct definitions, alternative, 53, 55
 - refined asymptotics, 65
 - finite state, 66
 - general, 65–66
- noiseless coding theorem *see* Average cost theorem; Average length theorem; noiseless channel
- Noisy channel coding theorem, 104
 - see also* discrete memoryless channel
- non-block code *see* variable length code
- non-cooperative source network, 397–398
- non-finite distortion measure, 117, 130
- non-interactive communication, 435
- Non-negativity lemma, 36
- normal channel network, 301
 - reduction to, 301–302
- normal source network (NSN), 254–261
 - auxiliary, 259
 - product space characterization of achievable rate region, 258
 - reduction to, 253
 - without helpers, 255
 - coding theorem, 257–258
 - error exponent, 269–270
 - universal coding, 269–270
 - with three inputs and one helper, 384–389
 - with two helpers, 389–390
- omniscience (OS, ε -OS), 436, 444
 - achievable rate, 436
- one side information source, 374–375
- one time pad, 401
- optimal code
 - fixed-to-variable length *see* Huffman code
 - variable-to-fixed length, 63
- optimal points, 247
- optimal transmission without coding, 118–119
- optimistic and pessimistic points of view, 93
 - for channel networks, 302
 - for channels, 93
 - for source networks, 261
 - for sources, 112
- oriented digraphs, 204
- output alphabet, xviii, 84, 272
- output constraint, 100–101
- output of a network, 250

Subject index

495

- output set, 83
 output vertex, 250
- P*-typical sequence, 20, 22
- Packing lemma, 145–147, 155, 159, 183
 simplified form, 160–161
- parallel channels *see* product of channels
- parity-check code *see* binary symmetric channel,
 linear code
- partial ordering
 of channels *see* comparison of channels
 of distributions *see* more uniform distribution
- partial side information, 361
 see also source coding with side information
- partitions, qualitatively independent, 200–202
- path, 250
- peak distortion measure, 117
- perfect graphs, 102
- perfect secrecy, 400, 401
- permutations, colliding, 206–207
- Pinsker inequality, 44
- polymatroid set function, 46
- polynomial coefficient, bounds on, 17, 26
- postulational characterization of entropy,
 12–13
- power digraphs, 194
- pragmatic approach, 22
- pre-channels, 301
- prefix code, 48, 59
 alphabetic, 62
 Kraft inequality 72–73
 optimal *see* Huffman code
 and search strategies, 61–62
 Shannon–Fano code, 49, 70
 synchronizing, 60
 tree representation, 49
- prefix property, 48
- privacy amplification, 413, 424, 443, 444
- private key (PK, ε -PK), 436
 achievable rates, 436, 440–442
 capacity *see* capacity, private key
- probability distributions, xiv
 ε -uniform, 401
- probability of correct decoding, non-achievable
 rates *see* exponential probability bounds
- probability of erasure, 155
- probability of error, xvii, 3, 83, 252
 average, 83, 154
 for family of channels, 154 172, 173
 fidelity criterion, xviii, 3, 115
 for source networks, 252
 hypothesis testing, 6
 maximum, 88, 154
 at output c , 252, 282, 283
 overall 94
 undetected, 155
 see also exponential probability bounds
- product
 of graphs *see* graph
 of channels, 98, 101
 of degraded broadcast channels, 376–379
 of sources, 117
- product space characterization, 262
- of achievable rate region, NSN, 258
- of channel network capacity region, 302
- pseudo information, 13
- public discussion in secrecy generation, 421–444,
 459
- Qualitative independence theorem, 202–203,
 207–208
- qualitatively independent partitions, 200–202
 Rényi problem, 207, 208
- quasi-image, 346–347
- r*-source *see* discrete memoryless multiple source
- random code, 214, 226–227
 capacity of an AVC, 227
 reduction lemma, 215
 realizability of, 214, 228
- random coding *see* random selection of
- random coding bound, 147
 alternative derivation, 178–179
 alternative form, 171
 BSC, 174
 linear codes, 179
 compound DMC, 155
 constant composition codes, 147–148
 improvement, 165–167
 universal, 163
 list codes, 175–176
 tightness for large rates, 150, 152
 for undetected error and erasure, 156, 164
 universal attainability of, 153–154, 156
 see also random coding exponent function
- random coding exponent function, 150, 152
 modified form, 156
 properties, 150, 151–152
 relation to sphere packing exponent function, 150
- random selection, method of, 132
- random selection of
 channel codes, 96–97
 codes (sources), 10–11
 extractors, 402
 fork network codes, 255
 MA codes, 288–289
 rate-slicing codes, 263–264
- random variables, xiv
 ε -recoverable, 421
 connected by a channel, 83
- randomized
 decoder *see* stochastic decoder
 encoder *see* stochastic encoder
 test, 9

- range constraint, auxiliary RVs, 310
 in computable characterizations, 262, 339
- rate
 achievable *see* achievable (ϵ -achievable) rate
 of channel block code, 84
 critical *see* critical rate
 Δ -distortion *see* Δ -distortion rate
 entropy rate, 51
 equivocation rate, 414
 of source block code, 107
 of variable length code, channel, 102
 pairs (MA code), 305
 triple (fork network code), 246
 vector (channel network code), 281
- rate-distortion function, 120
 alternative formula, 127–128
 channel achieving, 129
 computation of, 126–127, 129
 convexity, 108–109
 differentiability, 129
 joint continuity, 108
- Rate distortion theorem, 109–112
 application to coverings of product graphs 160
 arbitrarily varying source, 135, 140
 compound source, 139, 140
 multi-terminal generalizations, 366, 370–371, 392
 non-finite distortion measures, 117
 peak distortion measures, 117
 remote sources, 117–118
 two-step source coding, 392
 variable length codes, 118
 zero-error, 134
see also exponential probability bounds
- rate slicing
 corollary, 245–246
 limitations on, 376, 390
- reduction
 of channel network problems, 301–302
 of source network problems, 253–254
- redundancy, minimax, 68, 69, 130–131
- reliability function (of DMC), 152, 153
 bounds on, 177
 compound DMC, 154
 with feedback, 179–181
 generalized capacity as inverse of, 164
 list codes, 175–176
 at $R=0$, 169–170
 constant composition codes, 171
 rates above capacity, 165
 under input constraint, 162, 171
see also error exponent, DMC
- reliable transmission, xvi, xviii
 non-terminating, xix, 115
- remote sources, 118–119
- remainder terms *see* asymptotics, refined
- reproduction alphabet, 107
- row-convex closure, 210
- saturated code tree, 58
- search strategies and codes, 61–62
- secrecy
 ϵ -secrecy, 400, 401
 extraction *see* privacy amplification
 perfect, 400, 401
- Secrecy lemma, 405–407, 448, 459
- secrecy capacity, 424, 444, 459
 wiretap channel, 411–414
see also private key, capacity; secret key, capacity
- secret key (SK, ϵ -SK), 401, 421, 436
 achievable rates, 423
 capacity *see* capacity, secret key
 generation of
 channel model, basic, 422–424, 425, 426, 427
 multi-terminal channel model, 441–443
 multi-terminal source model, 435–443
 one-way source model, 427, 432–435
 source model, basic, 421–422, 423–427
- security index, 400–401, 458–459
 and communication protocols, 423
 properties of, 445
 and secret keys, 401, 421
 variational, 450
- self-information *see* information, provided by
 an event
- self-synchronizing code *see* synchronizing codes
- separable codes, 48
 composition of, 59
 Kraft inequality, generalized, 55, 59
 and prefix codes, 57
- separable range (of a code), 48
 algorithm to test, 59
- separation of source and channel coding, 114–115
 multi-terminal case, 288, 293
- sequence pairs
 joint type of, 17
 jointly typical, 20
- sequential encoder, 64
- Shannon
 block diagram, xvii, 113, 114–115
 codes, 51, 60, 67
 entropy *see* entropy
 formula, 4
 partial ordering of channels *see* ‘better in the Shannon sense’
- Shannon–Fano code, 70
- Shannon theory, ix
- shells, 18, 29
- side information (sources)
 code with, 244
 fork network with, 395–396
 partial, 361
 source of, 243, 361

- see also* source coding with side information
- single-letter characterization, 262, 264
- single-letter distortion measure *see* averaging
 - distortion measure
- Single-letterization lemma, 313
- size constraint *see* range constraint
- Slepian–Wolf network *see* fork network
- Slepian–Wolf theorem *see* Fork network coding theorem
- sliding block code, 64
- source, xvi
 - alphabet, 3
 - arbitrarily varying, 135, 140
 - compound, 139
 - component source of DMMS, 246
 - discrete memoryless (DMS), 3
 - multiple (DMMS), 243, 246
 - stationary, 51–52, 53, 58
 - entropy rate, 58–59
 - ergodic, 59, 60, 64–65
 - isomorphic, 64–65
 - see also* source coding theorems
- source-channel
 - block code, 113
 - coding theorem *see* source channel, transmission theorem
 - error exponent, 178
 - network (definition), 284
 - independent component sources, 293
 - transmission theorem, 113, 116
 - arbitrarily varying channels, 229–230
 - remote sources, 118
 - variable length codes, 118
- source coding theorems
 - block codes, 3, 10
 - with prescribed distortion level *see* Rate distortion theorem
 - multi-terminal *see* source coding with side information; source network coding theorems
 - variable length codes, 49, 53, 118
 - variable-to-fixed length codes, 63
 - see also* asymptotics refined; exponential probability bounds; universal coding
- source coding with side information, 244
 - partial side information, 361, 374
 - several decoders, 388
 - with prescribed distortion level, 363–365, 390
- source model of secret key generation *see* secret key, generation of
- source network, 251 ff
 - with 2 helpers, 388–390
 - with 3 inputs and 1 helper, 384–388
- achievable (ϵ -achievable) rate region, 252
 - probability of error fidelity criterion, 252–254
- arbitrary fidelity criteria, 369
 - auxiliary, 294, 200
 - coding theorems *see* source network coding theorems
 - of depth 2, 251, 253–254, 261, 263
 - of depth > 2, 271, 396
 - fork *see* fork network
 - non-cooperative, 397–399
 - one side information source, 374–376
 - with probability of error fidelity criterion
 - graphical representation, 251
 - reduction to NSN, 253, 254
 - zigzag, 384–5
 - see also* normal source network (NSN)
- source network coding theorems, 375–376, 384, 392, 395–396
 - and entropy characterization problem, 263, 268–269
 - fork network *see* fork network
 - NSN *see* normal source network
 - see also* source coding with side information
- Sperner capacity
 - digraph, 194
 - digraph family, 195
- Sperner family, 193
- Sperner’s theorem, 193, 204
- sphere packing bound, 148–150, 152
 - alternative derivations, 161–162, 171–173
 - BSC, 174
 - compound DMC, 154
 - constant composition codes, 148–150
 - improvement for small rates, 171–178
 - list codes, 176
 - tightness for large rates, 150, 151–152
 - under input constraint, 162
 - with feedback, 179
 - see also* sphere packing exponent function
- sphere packing exponent function, 148, 152
 - alternative form 192
 - compound DMC 173
 - properties, 150, 161
 - relation to random coding exponent function, 150
- standard minimum distance (SMD) decoder, 211
- state of a channel, 66–67, 209
 - see also* channel state information
- state selector, 222
- stationary source *see* source, stationary
- isomorphy problem, 65
- statistical hypotheses *see* hypothesis testing
- Stein’s lemma, 14
- stochastic decoding, 230
- stochastic encoder, 220
 - for BCC, 414, 415
 - effect on a - and m -capacity, AVC, 220–222
 - effect on a - and m -capacity region
 - general channel network, 292–293
 - MAC, 286–287

- and PK capacity, 442, 443
- for wiretap channel, 410
- stochastic matrix, xiv, xv, 73–75
 - doubly, 43
- stopping time, 62
- straight line bound, 177
- strong converse, 93, 94, 106
 - for channel codes from arbitrary sets, 90
 - exponential bound *see* exponential probability bounds
 - and image size problem, 359–360, 363, 384–388
 - invalidity of, 96, 163
 - see also under specific coding theorems*
- strong data processing lemma, 45, 345
- strongly typical sequences *see* typical sequences
- sub-achievable entropy vectors, 347–348
- subcode, 85
- subgraph, 102, 185, 204
 - induced, 102, 185, 194
- suffix code, 60
- sum-product algorithm, 94
- super-achievable entropy vectors, 350
- superposition coding, 357, 399, 459
- Support lemma, 310–311
- symbolic dynamics, 70
- symmetric
 - channel, 97
 - cliques, 194, 195, 196–197
 - joint distribution, 388
- synchronizing codes, 60
- test, statistical, 6
 - asymptotically optimal against all alternatives, 29–30
 - randomized, 9
 - see also* hypothesis testing
- time sharing principle, 247–248, 268, 288, 291, 296, 383, 389
 - lemma, 247–248, 274
- total communication, 435
- transinformation *see* mutual information
- transitive tournament, 204
- transmission
 - of independent sources, 288, 293
 - non-terminating, xviii–xix
 - reliable, xix, 115
- transmission ratio, xviii
 - see also* limit of minimum transmission ratio (LMTR)
- tree representation
 - codes, 49
 - variable-to-fixed length, 63
 - search strategies, 61–62
 - stopping times, 62, 63
- triangle, cyclic, 204
- trifference, 176
- turbo codes, 94, 106
- Twin partitions lemma, 192–193, 196
- two-input two-output MAC, 288–290
- two-observer DMC, 298–299
- two-output BC *see* broadcast channel
- two-source DMMS, 243
- two-step source coding, 392
- two-way channel, 291–292
 - unrestricted, 300–301
- type, 16 ff
 - class, 16
 - conditional, 18
 - joint, 17
- Type counting lemma, 16
- Type covering lemma, 132–134, 135, 136
- typical sequences, 20 ff, 407–410
 - delta-convention, 21
 - weakly *see* entropy-typical sequences
- Typicality lemma, 408–409
- unbiased estimator, 14
- uncertainty, xxi, 4
- undetected error, 155–156
 - joint bounds on probability of erasure and u. e., 156, 164
 - zero u. e. capacity, 179
- undirected graph, 194, 195
- uniquely decipherable code *see* separable codes
- uniquely decodable code *see* separable codes
- universal coding, 25, 56, 153–154, 159
 - channels, 154, 156, 162–163
 - sources
 - block codes, 23
 - variable length codes, 56–57
 - with a distortion measure, 137–138
 - source networks, 266–270
 - see also* universally attainable error exponent; universally optimal codes
- universal hash family, 11
- universal improvement on the random coding bound, 163
- universal variable-length codes, 67–70
- universally attainable error exponent channels, 153–154, 163
 - maximal, 154
- pair of, 156
- sources, 23, 137
- source networks, 266, 269–270
- universally optimal codes, 162
 - for sources, 25, 56–57, 67–70
 - with a distortion measure, 137–138
 - non-existence for channels, 162–163
- unrestricted image size problem, 341
- unrestricted models of generating SK, 422
- unrestricted two-way channel, 300–301
- V-shell, 18
- variable length codes

Subject index

499

- channels, 102–103
 - with feedback, 104, 181–182
- sources, 48 ff
 - general fidelity criteria, 118
 - variable-to-fixed-length codes, 63
 - universal, 67–70
 - see also* prefix code; separable codes
- variational distance *see* distance
- variational security index, 450
- vertex (of graph), 185, 189, 194, 250
- vertex packing polytope, 143
- weak converse, 93, 105
- weakly typical sequences *see* entropy-typical sequences
- weight of evidence, 7
- wiretap channel, 410–414, 444, 459
 - as channel model of generating SK, 422
 - secrecy capacity, 411, 424, 450, 452
 - see also* broadcast channel with confidential messages
- Wyner's common information, 394–395
- zero error capacity, 95
 - compound DMC, 186–189, 193
 - with informed decoder, 163, 187, 206, 265, 289
 - and expurgated bound, 167–168
 - with feedback, 104, 235
 - and sphere packing bound, 179
 - and graphs, 101–102
 - and m-capacity of AVCs, 225–226
 - list code, 176
 - region
 - adder MAC, 285
 - deterministic broadcast channel, 385
 - zero undetected error capacity, 179
- zero error code, for DMC, 184
 - cardinality, 184, 185
- zero error Δ -distortion rate, 116, 134
 - computation of, 140
- zero error rate region, 265
- zigzag source network, 384–385