Large Sets of Disjoint Packings And Large Sets of Disjoint GDDs

by

Demeng Chen

A Thesis
Submitted to the Faculty of Graduate Studies
in Partial Fulfillment of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba

(c) August, 1994

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

THE AUTHOR HAS GRANTED AN IRREVOCABLE NON-EXCLUSIVE LICENCE ALLOWING THE NATIONAL LIBRARY OF CANADA TO REPRODUCE, LOAN, DISTRIBUTE OR SELL COPIES OF HIS/HER THESIS BY ANY MEANS AND IN ANY FORM OR FORMAT, MAKING THIS THESIS AVAILABLE TO INTERESTED PERSONS.

L'AUTEUR A ACCORDE UNE LICENCE IRREVOCABLE ET NON EXCLUSIVE PERMETTANT A LA BIBLIOTHEQUE NATIONALE DU CANADA DE REPRODUIRE, PRETER, DISTRIBUER OU VENDRE DES COPIES DE SA THESE DE QUELQUE MANIERE ET SOUS QUELQUE FORME QUE CE SOIT POUR METTRE DES EXEMPLAIRES DE CETTE THESE A LA DISPOSITION DES PERSONNE INTERESSEES.

THE AUTHOR RETAINS OWNERSHIP OF THE COPYRIGHT IN HIS/HER THESIS. NEITHER THE THESIS NOR SUBSTANTIAL EXTRACTS FROM IT MAY BE PRINTED OR OTHERWISE REPRODUCED WITHOUT HIS/HER PERMISSION.

L'AUTEUR CONSERVE LA PROPRIETE DU DROIT D'AUTEUR QUI PROTEGE SA THESE. NI LA THESE NI DES EXTRAITS SUBSTANTIELS DE CELLE-CI NE DOIVENT ETRE IMPRIMES OU AUTREMENT REPRODUITS SANS SON AUTORISATION.

ISBN 0-315-99034-1

Canada

Name Chen Demeng

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

Combinatorics, Block Design
SUBJECT TERM

0405
SUBJECT CODE

U·M·I

Subject Categories

THE HUMANITIES AND SOCIAL SCIENCES

COMMUNICATIONS AND THE ARTS
Architecture 0729
Art History 0377
Cinema 0900
Dance 0378
Fine Arts 0357
Information Science 0723
Journalism 0391
Library Science 0399
Mass Communications 0708
Music 0413
Speech Communication 0459
Theater 0465

EDUCATION
General 0515
Administration 0514
Adult and Continuing 0516
Agricultural 0517
Art 0273
Bilingual and Multicultural 0282
Business 0688
Community College 0275
Curriculum and Instruction 0727
Early Childhood 0518
Elementary 0524
Finance 0277
Guidance and Counseling 0519
Health 0680
Higher 0745
History of 0520
Home Economics 0278
Industrial 0521
Language and Literature 0279
Mathematics 0280
Music 0522
Philosophy of 0998
Physical 0523
Psychology 0525
Reading 0535
Religious 0527
Sciences 0714
Secondary 0533
Social Sciences 0534
Sociology of 0340
Special 0529
Teacher Training 0530
Technology 0710
Tests and Measurements 0288
Vocational 0747

LANGUAGE, LITERATURE AND LINGUISTICS
Language
- General 0679
- Ancient 0289
- Linguistics 0290
- Modern 0291

Literature
- General 0401
- Classical 0294
- Comparative 0295
- Medieval 0297
- Modern 0298
- African 0316
- American 0591
- Asian 0305
- Canadian (English) 0352
- Canadian (French) 0355
- English 0593
- Germanic 0311
- Latin American 0312
- Middle Eastern 0315
- Romance 0313
- Slavic and East European 0314

PHILOSOPHY, RELIGION AND THEOLOGY
Philosophy 0422
Religion
- General 0318
- Biblical Studies 0321
- Clergy 0319
- History of 0320
- Philosophy of 0322

Theology 0469

SOCIAL SCIENCES
American Studies 0323
Anthropology
- Archaeology 0324
- Cultural 0326
- Physical 0327

Business Administration
- General 0310
- Accounting 0272
- Banking 0770
- Management 0454
- Marketing 0338

Canadian Studies 0385
Economics
- General 0501
- Agricultural 0503
- Commerce-Business 0505
- Finance 0508
- History 0509
- Labor 0510
- Theory 0511

Folklore 0358
Geography 0366
Gerontology 0351
History
- General 0578
- Ancient 0579
- Medieval 0581
- Modern 0582
- Black 0328
- African 0331
- Asia, Australia and Oceania 0332
- Canadian 0334
- European 0335
- Latin American 0336
- Middle Eastern 0333
- United States 0337

History of Science 0585
Law 0398
Political Science
- General 0615
- International Law and Relations 0616
- Public Administration 0617

Recreation 0814
Social Work 0452
Sociology
- General 0626
- Criminology and Penology 0627
- Demography 0938
- Ethnic and Racial Studies 0631
- Individual and Family Studies 0628
- Industrial and Labor Relations 0629
- Public and Social Welfare 0630
- Social Structure and Development 0700
- Theory and Methods 0344

Transportation 0709
Urban and Regional Planning 0999
Women's Studies 0453

THE SCIENCES AND ENGINEERING

BIOLOGICAL SCIENCES
Agriculture
- General 0473
- Agronomy 0285
- Animal Culture and Nutrition 0475
- Animal Pathology 0476
- Food Science and Technology 0359
- Forestry and Wildlife 0478
- Plant Culture 0479
- Plant Pathology 0480
- Plant Physiology 0817
- Range Management 0777
- Wood Technology 0746

Biology
- General 0306
- Anatomy 0287
- Biostatistics 0308
- Botany 0309
- Cell 0379
- Ecology 0329
- Entomology 0353
- Genetics 0369
- Limnology 0793
- Microbiology 0410
- Molecular 0307
- Neuroscience 0317
- Oceanography 0416
- Physiology 0433
- Radiation 0821
- Veterinary Science 0778
- Zoology 0472

Biophysics
- General 0786
- Medical 0760

EARTH SCIENCES
Biogeochemistry 0425
Geochemistry 0996
Geodesy 0370
Geology 0372
Geophysics 0373
Hydrology 0388
Mineralogy 0411
Paleobotany 0345
Paleoecology 0426
Paleontology 0418
Paleozoology 0985
Palynology 0427
Physical Geography 0368
Physical Oceanography 0415

HEALTH AND ENVIRONMENTAL SCIENCES
Environmental Sciences 0768
Health Sciences
- General 0566
- Audiology 0300
- Chemotherapy 0992
- Dentistry 0567
- Education 0350
- Hospital Management 0769
- Human Development 0758
- Immunology 0982
- Medicine and Surgery 0564
- Mental Health 0347
- Nursing 0569
- Nutrition 0570
- Obstetrics and Gynecology 0380
- Occupational Health and Therapy 0354
- Ophthalmology 0381
- Pathology 0571
- Pharmacology 0419
- Pharmacy 0572
- Physical Therapy 0382
- Public Health 0573
- Radiology 0574
- Recreation 0575
- Speech Pathology 0460
- Toxicology 0383

Home Economics 0386

PHYSICAL SCIENCES
Pure Sciences
Chemistry
- General 0485
- Agricultural 0749
- Analytical 0486
- Biochemistry 0487
- Inorganic 0488
- Nuclear 0738
- Organic 0490
- Pharmaceutical 0491
- Physical 0494
- Polymer 0495
- Radiation 0754

Mathematics 0405
Physics
- General 0605
- Acoustics 0986
- Astronomy and Astrophysics 0606
- Atmospheric Science 0608
- Atomic 0748
- Electronics and Electricity 0607
- Elementary Particles and High Energy 0798
- Fluid and Plasma 0759
- Molecular 0609
- Nuclear 0610
- Optics 0752
- Radiation 0756
- Solid State 0611

Statistics 0463

Applied Sciences
Applied Mechanics 0346
Computer Science 0984
Engineering
- General 0537
- Aerospace 0538
- Agricultural 0539
- Automotive 0540
- Biomedical 0541
- Chemical 0542
- Civil 0543
- Electronics and Electrical 0544
- Heat and Thermodynamics 0348
- Hydraulic 0545
- Industrial 0546
- Marine 0547
- Materials Science 0794
- Mechanical 0548
- Metallurgy 0743
- Mining 0551
- Nuclear 0552
- Packaging 0549
- Petroleum 0765
- Sanitary and Municipal 0554
- System Science 0790

Geotechnology 0428
Operations Research 0796
Plastics Technology 0795
Textile Technology 0994

PSYCHOLOGY
General 0621
Behavioral 0384
Clinical 0622
Developmental 0620
Experimental 0623
Industrial 0624
Personality 0625
Physiological 0989
Psychobiology 0349
Psychometrics 0632
Social 0451

Nom _____

Dissertation Abstracts International est organisé en catégories de sujets. Veuillez s.v.p. choisir le sujet qui décrit le mieux votre thèse et inscrivez le code numérique approprié dans l'espace réservé ci-dessous.

_____ ☐☐☐ U·M·I

SUJET — CODE DE SUJET

Catégories par sujets

HUMANITÉS ET SCIENCES SOCIALES

COMMUNICATIONS ET LES ARTS
Architecture 0729
Beaux-arts 0357
Bibliothéconomie 0399
Cinéma 0900
Communication verbale 0459
Communications 0708
Danse 0378
Histoire de l'art 0377
Journalisme 0391
Musique 0413
Sciences de l'information 0723
Théâtre 0465

ÉDUCATION
Généralités 515
Administration 0514
Art 0273
Collèges communautaires 0275
Commerce 0688
Économie domestique 0278
Éducation permanente 0516
Éducation préscolaire 0518
Éducation sanitaire 0680
Enseignement agricole 0517
Enseignement bilingue et multiculturel 0282
Enseignement industriel 0521
Enseignement primaire. 0524
Enseignement professionnel 0747
Enseignement religieux 0527
Enseignement secondaire 0533
Enseignement spécial 0529
Enseignement supérieur 0745
Évaluation 0288
Finances 0277
Formation des enseignants 0530
Histoire de l'éducation 0520
Langues et littérature 0279
Lecture 0535
Mathématiques 0280
Musique 0522
Orientation et consultation 0519
Philosophie de l'éducation 0998
Physique 0523
Programmes d'études et enseignement 0727
Psychologie 0525
Sciences 0714
Sciences sociales 0534
Sociologie de l'éducation 0340
Technologie 0710

LANGUE, LITTÉRATURE ET LINGUISTIQUE
Langues
- Généralités 0679
- Anciennes 0289
- Linguistique 0290
- Modernes 0291

Littérature
- Généralités 0401
- Anciennes 0294
- Comparée 0295
- Médiévale 0297
- Moderne 0298
- Africaine 0316
- Américaine 0591
- Anglaise 0593
- Asiatique 0305
- Canadienne (Anglaise) 0352
- Canadienne (Française) 0355
- Germanique 0311
- Latino-américaine 0312
- Moyen-orientale 0315
- Romane 0313
- Slave et est-européenne 0314

PHILOSOPHIE, RELIGION ET THÉOLOGIE
Philosophie 0422
Religion
- Généralités 0318
- Clergé 0319
- Études bibliques 0321
- Histoire des religions 0320
- Philosophie de la religion 0322

Théologie 0469

SCIENCES SOCIALES
Anthropologie
- Archéologie 0324
- Culturelle 0326
- Physique 0327

Droit 0398
Économie
- Généralités 0501
- Commerce-Affaires 0505
- Économie agricole 0503
- Économie du travail 0510
- Finances 0508
- Histoire 0509
- Théorie 0511

Études américaines 0323
Études canadiennes 0385
Études féministes 0453
Folklore 0358
Géographie 0366
Gérontologie 0351
Gestion des affaires
- Généralités 0310
- Administration 0454
- Banques 0770
- Comptabilité 0272
- Marketing 0338

Histoire
- Histoire générale 0578
- Ancienne 0579
- Médiévale 0581
- Moderne 0582
- Histoire des noirs 0328
- Africaine 0331
- Canadienne 0334
- États-Unis 0337
- Européenne 0335
- Moyen-orientale 0333
- Latino-américaine 0336
- Asie, Australie et Océanie 0332

Histoire des sciences 0585
Loisirs 0814
Planification urbaine et régionale 0999
Science politique
- Généralités 0615
- Administration publique 0617
- Droit et relations internationales 0616

Sociologie
- Généralités 0626
- Aide et bien-être social 0630
- Criminologie et établissements pénitentiaires 0627
- Démographie 0938
- Études de l' individu et de la famille 0628
- Études des relations interethniques et des relations raciales 0631
- Structure et développement social 0700
- Théorie et méthodes. 0344
- Travail et relations industrielles 0629

Transports 0709
Travail social 0452

SCIENCES ET INGÉNIERIE

SCIENCES BIOLOGIQUES
Agriculture
- Généralités 0473
- Agronomie. 0285
- Alimentation et technologie alimentaire 0359
- Culture 0479
- Élevage et alimentation 0475
- Exploitation des pâturages 0777
- Pathologie animale 0476
- Pathologie végétale 0480
- Physiologie végétale 0817
- Sylviculture et faune 0478
- Technologie du bois 0746

Biologie
- Généralités 0306
- Anatomie 0287
- Biologie (Statistiques) 0308
- Biologie moléculaire 0307
- Botanique 0309
- Cellule 0379
- Écologie 0329
- Entomologie 0353
- Génétique 0369
- Limnologie 0793
- Microbiologie 0410
- Neurologie 0317
- Océanographie 0416
- Physiologie 0433
- Radiation 0821
- Science vétérinaire 0778
- Zoologie 0472

Biophysique
- Généralités 0786
- Medicale 0760

SCIENCES DE LA TERRE
Biogéochimie 0425
Géochimie 0996
Géodésie 0370
Géographie physique 0368
Géologie 0372
Géophysique 0373
Hydrologie 0388
Minéralogie 0411
Océanographie physique 0415
Paléobotanique 0345
Paléoécologie 0426
Paléontologie 0418
Paléozoologie 0985
Palynologie 0427

SCIENCES DE LA SANTÉ ET DE L'ENVIRONNEMENT
Économie domestique 0386
Sciences de l'environnement 0768
Sciences de la santé
- Généralités 0566
- Administration des hôpitaux 0769
- Alimentation et nutrition 0570
- Audiologie 0300
- Chimiothérapie 0992
- Dentisterie 0567
- Développement humain 0758
- Enseignement 0350
- Immunologie 0982
- Loisirs 0575
- Médecine du travail et thérapie 0354
- Médecine et chirurgie 0564
- Obstétrique et gynécologie 0380
- Ophtalmologie 0381
- Orthophonie 0460
- Pathologie 0571
- Pharmacie 0572
- Pharmacologie 0419
- Physiothérapie 0382
- Radiologie 0574
- Santé mentale 0347
- Santé publique 0573
- Soins infirmiers 0569
- Toxicologie 0383

SCIENCES PHYSIQUES
Sciences Pures
Chimie
- Généralités 0485
- Biochimie 487
- Chimie agricole 0749
- Chimie analytique 0486
- Chimie minérale 0488
- Chimie nucléaire 0738
- Chimie organique 0490
- Chimie pharmaceutique 0491
- Physique 0494
- PolymÈres 0495
- Radiation 0754

Mathématiques 0405
Physique
- Généralités 0605
- Acoustique 0986
- Astronomie et astrophysique 0606
- Électronique et électricité 0607
- Fluides et plasma 0759
- Météorologie 0608
- Optique 0752
- Particules (Physique nucléaire) 0798
- Physique atomique 0748
- Physique de l'état solide 0611
- Physique moléculaire 0609
- Physique nucléaire 0610
- Radiation 0756

Statistiques 0463

Sciences Appliqués Et Technologie
Informatique 0984
Ingénierie
- Généralités 0537
- Agricole 0539
- Automobile 0540
- Biomédicale 0541
- Chaleur et thermodynamique 0348
- Conditionnement (Emballage) 0549
- Génie aérospatial 0538
- Génie chimique 0542
- Génie civil 0543
- Génie électronique et électrique 0544
- Génie industriel 0546
- Génie mécanique 0548
- Génie nucléaire 0552
- Ingénierie des systèmes 0790
- Mécanique navale 0547
- Métallurgie 0743
- Science des matériaux 0794
- Technique du pétrole 0765
- Technique minière 0551
- Techniques sanitaires et municipales 0554
- Technologie hydraulique 0545

Mécanique appliquée 0346
Géotechnologie 0428
Matières plastiques (Technologie) 0795
Recherche opérationnelle 0796
Textiles et tissus (Technologie) 0794

PSYCHOLOGIE
Généralités 0621
Personnalité 0625
Psychobiologie 0349
Psychologie clinique 0622
Psychologie du comportement 0384
Psychologie du développement 0620
Psychologie expérimentale 0623
Psychologie industrielle 0624
Psychologie physiologique 0989
Psychologie sociale 0451
Psychométrie 0632

LARGE SETS OF DISJOINT PACKINGS AND LARGE SETS OF DISJOINT GDDs

BY

DEMENG CHEN

A Thesis submitted to the Faculty of Graduate Studies of the University of Manitoba in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

© 1994

Permission has been granted to the LIBRARY OF THE UNIVERSITY OF MANITOBA to lend or sell copies of this thesis, to the NATIONAL LIBRARY OF CANADA to microfilm this thesis and to lend or sell copies of the film, and UNIVERSITY MICROFILMS to publish an abstract of this thesis.

The author reserves other publications rights, and neither the thesis nor extensive extracts from it may be printed or otherwise reproduced without the author's permission.

Abstract

A (2, 3)-packing on X is a pair (X, $\mathcal{B}$), where X is a set of v points, and $\mathcal{B}$ is a set of 3-subsets of X called blocks, such that every pair of points appears in at most one block. The leave of a (2, 3)-packing (X, $\mathcal{B}$) is the graph (X, E), where E consists of all the pairs which do not appear in any block of $\mathcal{B}$. Two (or more) (2,3)-packings are said to be compatible if they have the same leave. Two (or more) (2,3)-packings are said to be disjoint if they have disjoint block sets. One of the two topics of this thesis is to construct the maximum number of disjoint compatible (2,3)-packings.

The other topic is to construct the maximum number of disjoint compatible 3-GDD. A 3-GDD is a group-divisible design (GDD) with block size 3. A group-divisible design is a triple (X, $\mathcal{G}$, $\mathcal{B}$), where

1) X is a finite set of points,
2) $\mathcal{G}$ is a partition of X into subsets called groups,
3) $\mathcal{B}$ is a set of subsets of X called blocks, such that no block intersects any group in more than one point, and every two points from two distinct groups appear in a unique block.

Two (or more) 3-GDD are said to be compatible if they have the same group set. Two (or more) 3-GDD are said to be disjoint if their block sets are disjoint.

These two topics are closely related to each other and mutually useful. This thesis gives a series of construction techniques and new results on these two topics.

Acknowledgments

Firstly, I want to express my gratitude to members of my thesis committee for their patience and many suggestions.

Secondly, I want to thank Dr. D. R. Stinson for his guidance and financial support in the form of scholarship. Major part of this thesis was done under his two years supervision. Thank you is also extended to Dr. R. G. Stanton who supervised me for the rest three years, and whose help is essential to complete this work.

Thirdly, thanks goes to my wife Haiyan for her support, understanding and love.

Finally, I thank the University of Manitoba for providing me the opportunity to study here and for the financial support in the form of Graduate Fellowship.

TABLE OF CONTENTS

		page
Abstract		iv
Acknowledgments		v
Chapter 1	Large Sets of Disjoint (2,3)-packings	1
1.1	Introduction	1
1.2	The concept and the problem	1
1.3	Known results	2
Chapter 2	Large Sets of Disjoint Group-Divisible Designs	4
2.1	Introduction	4
2.2	The concept and the problem	4
2.3	Known results	5
Chapter 3	Constructions Using Large Sets And Prime Numbers	7
3.1	Introduction	7
3.2	Construction I	7
3.3	More GLS(v)	10
3.4	Construction II	16
3.5	Construction III	24
Chapter 4	Tripling Constructions	30
4.1	Introduction	30
4.2	Preliminaries	30
4.3	Construction I	31
4.4	Construction II	33
Chapter 5	The Doubling Construction	36
5.1	Introduction	36
5.2	Preliminaries	36

5.3	The main construction	38
5.4	A lemma about one-factorization	42
5.5	Results on LA(t^u)	45
5.6	Summary of this chapter	50
Chapter 6	Another Tripling Construction	51
6.1	Introduction	51
6.2	Preliminaries	51
6.3	The auxiliary design	53
6.4	The use of the auxiliary design	55
6.5	Construction for 4-AD(1,v)	58
6.6	Some small examples of 4-AD(1,v)	62
6.7	Summary of the chapter	66
Chapter 7	Summarizing Results	68
7.1	Introduction	68
7.2	Summary of recursive results	68
7.3	Summary of results about MP(v)	69
References		71
Appendix I		74
Appendix II	77	

Chapter 1

Large Sets of Disjoint (2,3)-packings

1.1 Introduction

This thesis deals with two topics. One of them, large sets of disjoint (2,3)-packings, is introduced in this chapter. The other one is introduced in chapter two.

1.2 The concept and the problem

Suppose X is a set of v elements called *points*. A *(2, 3)-packing* on X is a pair (X, $\mathcal{B}$), where $\mathcal{B}$ is a set of 3-subsets of X called *blocks*, such that every pair of points appears in at most one block. If $|X| = v$, a (2, 3)-packing on X is said to be *of order v*. The *leave* of a (2, 3)-packing (X, $\mathcal{B}$) is the graph (X, E), where E consists of all the pairs which do not appear in any block of $\mathcal{B}$. A (2, 3)-packing (X, $\mathcal{B}$) is said to be *maximum* if there does not exist any (2,3)-packing (X, $\mathcal{A}$) such that $|\mathcal{A}| > |\mathcal{B}|$. From now on, we restrict our attention to (2, 3)-packings on v points in which every point occurs in at least one block (since, if there are points that occur in no blocks, then we have a (2, 3)-packing on v' points for some $v' < v$).

Two (or more) (2,3)-packings are said to be *compatible* if they have the same leave. Two (2,3)-packings (X, $\mathcal{A}$) and (X, $\mathcal{B}$) are said to be *disjoint* if $\mathcal{A} \cap \mathcal{B} = \emptyset$. A set of (2,3)-packings is said to be *disjoint* if every pair is disjoint. From now on, disjoint (2,3)-packings are assumed to be compatible, if not otherwise stated.

Example. ([25]) Let $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. The following are 4 disjoint (2, 3)-packings $(X, \mathcal{A}_i)$, $1 \le i \le 4$. All of them have the leave consisting of one-factor $\{\{1, 5\}, \{2, 6\}, \{3, 7\}, \{4, 8\}\}$.

$(X, \mathcal{A}_1)$:	$(X, \mathcal{A}_2)$:	$(X, \mathcal{A}_3)$:	$(X, \mathcal{A}_4)$:
{1, 2, 3}	{2, 3, 4}	{3, 4, 5}	{4, 5, 6}
{5, 6, 7}	{6, 7, 8}	{7, 8, 1}	{8, 1, 2}
{1, 4, 7}	{2, 5, 8}	{3, 6, 1}	{4, 7, 2}

{5, 8, 3}	{6, 1, 4}	{7, 2, 5}	{8, 3, 6}
{1, 6, 8}	{2, 7, 1}	{3, 8, 2}	{4, 1, 3}
{5, 2, 4}	{6, 3, 5}	{7, 4, 6}	{8, 5, 7}
{2, 7, 8}	{3, 8, 1}	{4, 1, 2}	{5, 2, 3}
{6, 3, 4}	{7, 4, 5}	{8, 5, 6}	{1, 6, 7}

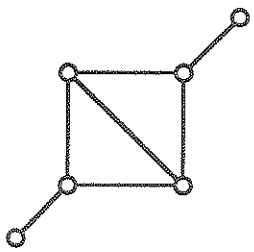
Let MP(v) be the maximum number of disjoint (2,3)-packings on v points. MP(v) are first used in [28] (Stinson and Vanstone) and [25] (Schellenberg and Stinson) to construct perfect threshold schemes. From the above example, MP(8) $\geq$ 4. A natural question is, what is the value of MP(v) for v $\geq$ 6.

The following upper bound of MP(v) is from [25].

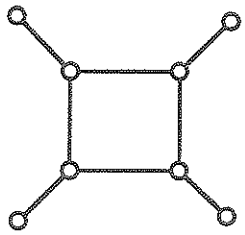
Theorem 1.2.1 ([25]) (1) If v $\equiv$ 1 or 3 (mod 6), MP(v) $\leq$ v - 2; the upper bound is attained only if the (2,3)-packings are maximum.
(2) If v $\equiv$ 0, 2 or 5 (mod 6), MP(v) $\leq$ v - 4; the upper bound is attained only if the (2,3)-packings are maximum.
(3) If v $\equiv$ 4 (mod 6), MP(v) $\leq$ v - 6; the upper bound is attained only if the (2,3)-packings have the same leave which is isomorphic to one of the four graphs:

$K_{1,3} \cup ((v - 4) / 2) K_2$ $\qquad$ $K_4 \cup ((v - 4) / 2) K_2$
$G_1 \cup ((v - 6) / 2) K_2$ $\qquad$ $G_2 \cup ((v - 8) / 2) K_2$

where G_1 and G_2 are as follows.



G_1



G_2

If MP(v) reaches the upper bound of Teorem 1.2.1, then a set of MP(v) disjoint (2,3)-packings on v points is called *a large set of disjoint (2, 3)-packings* of order v or simply *a*

large set, denoted by LSDP(v). One of the two purposes of this thesis is to construct LSDP(v).

1.3 Known results

This section presents some known results about (2, 3)-packings and some MP(v).

The number D(2, 3, v) is defined to be the number of blocks in a maximum (2, 3)-packing of order v. The follow result is well known. For convenience we state it as

Theorem 1.3.1 ([26][27]) (1) If $v \equiv 1$ or 3 (mod 6), then $D(2, 3, v) = v(v - 1) / 6$. The leave of such a maximum (2, 3)-packing is $(K_v)^c$.
(2) If $v \equiv 5$ (mod 6), then $D(2, 3, v) = (v(v - 1) - 8) / 6$. The leave of such a maximum (2, 3)-packing is a 4-cycle.
(3) If $v \equiv 0$ or 2 (mod 6), then $D(2, 3, v) = v(v - 2) / 6$. The leave of such a maximum (2, 3)-packing is a one-factor.
(4) If $v \equiv 4$ (mod 6), then $D(2, 3, v) = (v(v - 2) - 2) / 6$. The leave of such a maximum (2, 3)-packing is the disjoint union of $(v - 4) / 2$ edges and one $K_{1,3}$.

For $v \equiv 1$ or 3 (mod 6), a maximum (2,3)-packing of order v is called a *Steiner triple system* of order v (briefly, STS(v)). An STS(v) exists if and only if $v \equiv 1$ or 3 (mod 6). Any two STS(v) are compatible. Therefore, for above v, an LSDP(v) is *a large set of disjoint Steiner triple systems*, whose existence is now completely settled (see [20], [21] and [30]). The result is $MP(v) = v - 2$, i.e., the upper bound is reached, if $v \equiv 1$ or 3 (mod 6), $v > 7$. $MP(7) = 3$ is obtained in Example 4.5 of [25]. For later use, we specifically denote a large set of disjoint Steiner triple system of order v by LS(v).

For $v \equiv 0$ or 2 (mod 12), $MP(v) = v - 4$ ([25]). For $v \equiv 4, 5, 6, 8, 10, 11$ (mod 12), the value of MP(v) remains open except $MP(6) = 2$, $MP(8) = 4$, $MP(10) = 4$, $MP(11) = 7$ ([25]). This thesis will give more values of MP(v). The results are summarized in Theorem 7.3.3 and Theorem 7.3.4. Note that if MP(v) reaches the upper bound in Theorem 1,2,1, there exists an LSDP(v).

Chapter 2

Large Sets of Disjoint Group-Divisible Designs

2.1 Introduction

This chapter introduces the second topic of this thesis, that is, large sets of disjoint group-divisible designs.

2.2 The concept and the problem

A *group divisible design* (GDD) is a convenient tool as well as an interesting topic in combinatorial designs. A GDD is a triple (X, $\mathcal{G}$, $\mathcal{B}$) such that

1) X is a finite set of *points*,
2) $\mathcal{G}$ is a partition of X into subsets called *groups*,
3) $\mathcal{B}$ is a set of subsets of X called *blocks*, such that no block intersects any group in more than one point, and every two points from two distinct groups appear in a unique block.

The *type* of a GDD is denoted by $t^i s^j \ldots$, if there are i groups of size t, j of size s, and so on. A GDD with block size 3 is called a *3-GDD*. A 3-GDD of type T is denoted by 3-GDD(T). A *parallel class* of a GDD is a subset of blocks which forms a partition of X. If the block set itself can be partitioned into parallel classes, then the GDD is said to be *resolvable*.

Two (or more) 3-GDD(T) are said to be *compatible* if they have the same group set. Two 3-GDD(T) are said to be *disjoint* if their block sets are disjoint. A set of more than two 3-GDD(T) are said to be *disjoint* if each pair is disjoint. From now on, disjoint 3-GDD(T) are assumed to be compatible, if not otherwise stated.

A set of maximum number of disjoint 3-GDD(T) is called *a large set of disjoint 3-GDD(T)* or simply *a large set,* and is denoted by LSDG(T).

Suppose $s \geq t$; it is easy to prove that the maximum number of disjoint 3-GDD($t^u s^1$) ($s \geq t$) does not exceed $t(u - 1)$. A set of $t(u - 1)$ disjoint 3-GDD($t^u s^1$) must then be a large set.

A 3-GDD $(X, \mathcal{G}, \mathcal{B})$ is equivalent to a (2, 3)-packing $(X, \mathcal{B})$ with a leave that is a disjoint union of cliques. For $u \equiv 0$ or 2 (mod 6), a 3-GDD($2^{u/2}$) is a maximum (2, 3)-packing of order u having a one-factor as the leave. Thus an LSDP(u) is an LSDG($2^{u/2}$). For $u \equiv 4$ (mod 6), a 3-GDD($2^{(u-4)/2}4^1$) is a (2, 3)-packing with leave $K_4 \cup ((u - 4) / 2) K_2$. Thus an LSDP(u) is an LSDG($2^{(u-4)/2}4^1$).

Besides constructing LSDP(v) or determining MP(v), the other purpose of this thesis is to construct LSDG($t^u s^1$) with $s \geq t$.

2.3 Known results

This section presents some known results about 3-GDD($t^u s^1$) and known results about LSDG($t^u s^1$) with $s \geq t$.

A 3-GDD($t^u s^1$) has $t^2u(u - 1) / 6 + stu / 3$ blocks. And each point in a group of size t is in $(t(u - 1) + s) / 2$ blocks, each point in the group of size s in $tu / 2$ blocks. So, the necessary conditions for the existence of a 3-GDD($t^u s^1$) are

$$t^2u(u - 1) + 2tus \equiv 0 \pmod 6,$$
$$t(u - 1) + s \equiv 0 \pmod 2,$$
$$tu \equiv 0 \pmod 2,$$
$$t(u-1) \geq s.$$

These conditions are proved sufficient (in [7]) for the existence of a 3-GDD($t^u s^1$).

A 3-GDD(1^u) is an STS(u). So, an LSDG(1^u) is a large set of disjoint Steiner triple systems, hence an LSDP(u), for $u \equiv 1$ or 3 (mod 6), $u > 7$. Other known results are given in the following three lemmas.

Lemma 2.3.1 There exists an LSDG(t^3) for $t > 0$.

Proof. Take an additive abelian group G of order t. Let $X = \{a, b, c\} \times G$ and let $\mathcal{G}$ consist of $\{a\} \times G$, $\{b\} \times G$ and $\{c\} \times G$. For any $x \in G$, define $\mathcal{B}_x = \{\{(a, i), (b, j), (c, k)\}: i + j + k = x\}$. Then $(X, \mathcal{G}, \mathcal{B}_x)$ is a 3-GDD(t^3). And $\mathcal{B}_x \cap \mathcal{B}_y = \emptyset$, for $x \neq y$, $x, y \in G$. Therefore, we have an LSDG(t^3). ♦

Lemma 2.3.2 Suppose t(u+1) is even. Then there exists an LSDG($t^{u+1}(tu)^1$).

Proof. Take a 3-GDD($t^{u+1}(tu)^1$) $(X, \mathcal{G}, \mathcal{B})$. Suppose G_0 is the group of size tu. Then every block intersects G_0 in one point. Let p be a permutation on G_0 that consists of a single cycle of length tu. For i, $0 \leq i \leq tu - 1$, define $(X, \mathcal{G}, \mathcal{B}_i)$ to be the 3-GDD obtained from $(X, \mathcal{G}, \mathcal{B})$ by applying p^i to G_0. It is easy to see that $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$, for $0 \leq i < j \leq tu - 1$. Therefore an LSDG($t^{u+1}(tu)^1$) is constructed. ♦

Lemma 2.3.3 Suppose there exists an LSDG($t^u s^1$), $s \geq t$. Then there exists an LSDG($(tw)^u(sw)^1$), $w > 0$.

Proof Suppose $(X, \mathcal{G}, \mathcal{B}_i)$, $1 \leq i \leq t(u - 1)$, form an LSDG($t^u s^1$). Let $Y = X \times Z_w$, let $\mathcal{H} = \{G \times Z_w: G \in \mathcal{G}\}$. From each $(X, \mathcal{G}, \mathcal{B}_i)$, we construct w 3-GDD($(tw)^u(sw)^1$) $(Y, \mathcal{H}, \mathcal{B}_{ij})$, $1 \leq j \leq w$, as follows. For $\{a, b, c\} \in \mathcal{B}_i$, take an LSDG($w^3$) on $\{a, b, c\} \times Z_w$ such that the groups are $\{a\} \times Z_w$, $\{b\} \times Z_w$ and $\{c\} \times Z_w$. Name the w block sets $\{a, b, c\}_j$, $1 \leq j \leq w$. Let $\mathcal{B}_{ij} = \cup \{a, b, c\}_j$, where the union is over the set $\{a, b, c\} \in \mathcal{B}_i$. Then $(Y, \mathcal{H}, \mathcal{B}_{ij})$, $1 \leq i \leq t(u - 1)$, $1 \leq j \leq w$, form an LSDG($(tw)^u(sw)^1$), $w > 0$. ♦

In the following chapters we will construct more LSDG($t^u s^1$) with $s \geq t$.

Chapter 3

Constructions Using Large Sets and Prime Numbers

Main results:

1. Suppose an LSDG(t^{u+2}) exists. Then an LSDG(t^{up+2}) exists, where p is a prime number and one of the following conditions is satisfied:
   1) $p \equiv 7 \pmod 8$;
   2) $p \equiv 1 \pmod 8$ and $p \leq 137$;
   3) $u \geq 5$, $p \equiv 5 \pmod 8$ and $p \leq 157$;
   4) $p = 19$.
2. Suppose t is even and an LSDG(t^{u+2}) exists. Then an LSDG($t^{u(v-2)+2}$) exists, where $v \equiv 1$ or $3 \pmod 6$, $v > 1$.

3.1 Introduction

This chapter gives three kinds of constructions for large set of disjoint 3-GDDs. The first uses *good* large sets of disjoint Steiner triple systems (section 3.2). The second uses large sets of disjoint Steiner triple systems (section 3.4). The third uses prime numbers (section 3.5). Some new good large sets of disjoint Steiner triple systems are given in section 3.3. The material in section 3.2 and section 3.4 has been published in [3].

3.2 Construction I

This section presents a recursive construction for LSDG(t^u). First we give a preliminary lemma.

Lemma 3.2.1 Suppose $v \equiv 1, 3 \pmod 6$. If there exists an LSDG(t^{u+2}), then there exist tu disjoint 3-GDD($t^{u(v-2)+2}$)s.

Proof. Let $(X, \mathcal{A})$ be an STS(v) on point set $X = \{\infty, \infty'\} \cup Z_{v-2}$. Suppose $\{\infty, \infty', z\} \in \mathcal{A}$. For $x \in X$, define $E(\mathcal{A}, x) = \{\{a, b\} : \{a, b, x\} \in \mathcal{A}\}$. Then $E(\mathcal{A}, \infty) \cup E(\mathcal{A}, \infty')$ forms a 2-regular graph on the point set $Z_{v-2} \setminus \{z\}$. Direct these edges so that every point has indegree one and outdegree one, and call the resulting collection of ordered pairs $D(\mathcal{A}, \infty, \infty')$.

We now proceed to construct tu disjoint 3-GDD($t^{u(v-2)+2}$)s. As the point set, take

$$Y = (\{\infty, \infty'\} \times Z_t) \cup (Z_{v-2} \times Z_u \times Z_t).$$

Let Group set $\mathcal{G}$ consist of the following $2 + (v - 2)u$ sets:

$$\{\infty\} \times Z_t,\ \{\infty'\} \times Z_t,\ \{i\} \times \{j\} \times Z_t\ (i \in Z_{v-2}, j \in Z_u).$$

The block sets are obtained as follows. For each block $A \in \mathcal{A}$ do the following.

1) If $A = \{a, b, c\}$, $a, b, c \in Z_{v-2}$, then take an LSDG($(tu)^3$) on point set $A \times Z_u \times Z_t$, with groups $\{a\} \times Z_u \times Z_t$, $\{b\} \times Z_u \times Z_t$, and $\{c\} \times Z_u \times Z_t$. (This exists by Lemma 2.3.1) Name the tu block sets $\mathcal{B}(A, j, k)$, $j \in Z_u$, $k \in Z_t$.
2) If $A = \{\infty, a, b\}$ and $(a, b) \in D(\mathcal{A}, \infty, \infty')$, take an LSDG($t^{u+1}(tu)^1$) on point set $(\{\infty\} \times Z_t) \cup (\{a, b\} \times Z_u \times Z_t)$, with groups $\{\infty\} \times Z_t$, $\{(a, j, k): k \in Z_t\}$ $(j \in Z_u)$, and $\{b\} \times Z_u \times Z_t$. (This exists by Lemma 2.3.2) Name the tu block sets $\mathcal{B}(A, j, k)$, $j \in Z_u$, $k \in Z_t$.
3) If $A = \{\infty', a, b\}$ and $(a, b) \in D(\mathcal{A}, \infty, \infty')$, then proceed as in (2), but replace ∞ by ∞' and take the groups to be $\{\infty'\} \times Z_t$, $\{(a, j, k) : k \in Z_t\}$ $(j \in Z_u)$, and $\{b\} \times Z_u \times Z_t$. As before, name the tu block sets $\mathcal{B}(A, j, k)$, $j \in Z_u$, $k \in Z_t$.
4) If $A = \{\infty, \infty', z\}$, then take an LSDG($t^{u+2}$) on point set $(\{\infty, \infty'\} \times Z_t) \cup (\{z\} \times Z_u \times Z_t)$, with groups $\{\infty\} \times Z_t$, $\{\infty'\} \times Z_t$, $\{(z, j, k) : k \in Z_t\}$ $(j \in Z_u)$. Name the block sets $\mathcal{B}(A, j, k)$, $j \in Z_u$, $k \in Z_t$.

For any $j \in Z_u$, $k \in Z_t$, define

$$\mathcal{B}(j, k) = \bigcup_{A \in \mathcal{A}} \mathcal{B}(A, j, k).$$

Then each $(Y, \mathcal{G}, \mathcal{B}(j, k))$ is a 3-GDD of type $t^{u(v-2)+2}$ and these 3-GDDs are disjoint. The verifications are straightforward. ♦

In order to construct an LSDG($t^{u(v-2)+2}$), we start with an LS(v), $v \equiv 1$ or 3 (mod 6), and apply the construction of the above lemma to each STS(v) in the large set. We obtain a total of tu(v - 2) 3-GDDs, which are disjoint if the LS(v) satisfies a special property that we now define.

Suppose we have an LS(v), $v \equiv 1$ or 3 (mod 6), on point set $X = \{\infty, \infty'\} \cup Z_{v-2}$. We can name the block sets $\mathcal{A}_i$ ($i \in Z_{v-2}$). For each $\mathcal{A}_i$, construct a set of ordered pairs $D(\mathcal{A}_i, \infty, \infty')$ as in the proof of Lemma 3.2.1. We say that $\mathcal{A}_i$ is *amicable* with $\mathcal{A}_j$ if

$$D(\mathcal{A}_i, \infty, \infty') \cap D(\mathcal{A}_j, \infty, \infty') = \varnothing.$$

A large set LS(v), $v \equiv 1$ or 3 (mod 6), is called a *good large set*, denoted by GLS(v), if it consists of mutually amicable block sets.

Lemma 3.2.2 Suppose there exist a GLS(v) and an LSDG(t^{u+2}). Then there exists an LSDG($t^{u(v-2)+2}$).

Proof. The only possible difficulty is that we could have a block {(a, j, k), (a, j', k'), (b, j", k")} occurring in two of the GDDs, say in the GDDs arising from $\mathcal{A}_i$ and $\mathcal{A}_{i'}$ ($i \neq i'$). But this would mean that $(a, b) \in D(\mathcal{A}_i, \infty, \infty') \cap D(\mathcal{A}_{i'}, \infty, \infty')$, which will not occur if we take a GLS(v). ♦

In view of Lemma 3.2.2, GLS(v) are of interest. GLS(v) were first defined and used by Lu [20] who proved the following.

Lemma 3.2.3 For a prime number $p \equiv 7$ mod 8, there exists a GLS(p+2).

Proof. We use the construction due to Wilson [36] and Schreiber [26]. Take point set

$$X = \{\infty, \infty'\} \cup Z_p.$$

For each $i \in Z_p$, define a set of blocks $\mathcal{A}_i$ consisting of the following:

1) $\{a, b, c\}$ if $a + b + c \equiv i$ (mod p) and $a \neq b \neq c \neq a$,
2) $\{\infty, a + i, -2a + i\}$ if a is a quadratic residue (mod p),

3) $\{\infty', a + i, -2a + i\}$ if a is a quadratic non-residue (mod p),

4) $\{\infty, \infty', i\}$.

Then $(X, \mathcal{A}_i)$ is a STS(v), and these p STS(v)s are disjoint. Now, for each $i \in Z_p$, define $D(\mathcal{A}_i, \infty, \infty') = \{(a + i, -2a + i) : a \neq 0\}$. Thus we get a GLS(p+2). ♦

From Lemma 3.2.2 and 3.2.3, we have the following.

Lemma 3.2.4 Suppose there exists an LSDG(t^{u+2}). Then there exists an LSDG(t^{up+2}) for any prime number $p \equiv 7 \bmod 8$.

Lu [20] also verified that a GLS(p+2) exists for p = 17 or 19. In the next section, we construct some more GLS(p+2) with $p \equiv 1 \bmod 8$.

3.3 More GLS(v)

In the following, we present some GLS(p+2) with prime $p \equiv 1 \pmod 8$. Before that, we give some lemmas which will be used in this section and later.

Let F_q be a finite field of odd order q. Let $F_q^* = F_q \setminus \{0\}$. Define $\mathcal{P}_3(F_q)$ to be the set of all 3-subsets of F_q. Suppose $a, b, c, d, e \in F_q$. Define $d + \{a, b, c\} = \{d + a, d + b, d + c\}$. Define $e\{a, b, c\} = \{ea, eb, ec\}$.

For $A, B \in \mathcal{P}_3(F_q)$, we say A *has relation* $\sim$ *with* B, denoted by $A \sim B$, if there exists $d \in F_q$, $e \in F_q^*$, such that $A = d + eB$.

Lemma 3.3.1 $\sim$ is an equivalence relation, that is, the following hold.

(i) $A \sim A$.
(ii) If $A \sim B$, then $B \sim A$.
(iii) If $A \sim B$ and $B \sim C$, then $A \sim C$.

Proof. The verification is simple. ♦

By Lemma 3.3.1, $\mathcal{P}_3(F_q)$ can be divided into equivalence classes. In the following, we give a description of each equivalence class.

For $\{a, b, c\} \in \mathcal{P}_3(F_q)$, there are six u's such that

$$\{a, b, c\} = d_u + e_u \{0, 1, u\}$$

for some $d_u \in F_q$ and $e_u \in F_q^*$. We denote the set of six u's (not necessary distinct) thus obtained by $U(\{a, b, c\})$ (briefly $U(a, b, c)$). $U(a, b, c)$ is called the *U-set* of $\{a, b, c\}$. It is obvious that $A \sim \{0, 1, u\}$ if $u \in U(A)$. We will show in the following that triples in the same equivalence class have the same U-set.

Lemma 3.3.2 $A \sim B$ if and only if $U(A) = U(B)$.

Proof. Suppose $U(A) = U(B)$. Take $u \in U(A)$. Then $A \sim \{0, 1, u\}$. Since $U(A) = U(B)$, $u \in U(B)$. Thus $B \sim \{0, 1, u\}$. Therefore, $A \sim B$.

Suppose $A \sim B$. Take $u \in U(A)$. Then $A \sim \{0, 1, u\}$. Hence $B \sim \{0, 1, u\}$. Thus, $u \in U(B)$. Therefore, $U(A) \subseteq U(B)$. In the same way $U(B) \subseteq U(A)$. Therefore $U(A) = U(B)$. ♦

Lemma 3.3.3 If $U(A) \neq U(B)$, then $U(A) \cap U(B) = \varnothing$.

Proof. If $u \in U(A) \cap U(B)$, then $A \sim \{0, 1, u\}$, $B \sim \{0, 1, u\}$. Thus $A \sim B$. Hence $U(A) = U(B)$. That is a contradiction. Therefore $U(A) \cap U(B) = \varnothing$. ♦

From the above, we know that blocks in the same equivalence class have the same U-set. Therefore a U-set can be viewed as being the U-set of the equivalence class. Furthermore, different equivalence classes have disjoint U-sets.

Now we check the size of each equivalence class. We denote the equivalence class containing A by $\langle A \rangle$. $\langle \{a, b, c\} \rangle$ is briefly denoted by $\langle a, b, c \rangle$. The size of $\langle A \rangle$ is denoted by $|\langle A \rangle|$.

Lemma 3.3.4 $|\langle 0, 1, -1 \rangle| = q(q - 1) / 2$ if $3 \neq 0$; $|\langle 0, 1, -1 \rangle| = q(q - 1) / 6$ if $3 = 0$.

Proof. All triples in class $\langle 0, 1, -1\rangle$ are of the form $d + e\{0, 1, -1\}$, $d \in F_q$ and $e \in F_q^*$. Suppose $(d, e) \neq (f, g)$, $d, f \in F_q$ and $e, g \in F_q^*$. If $3 \neq 0$, it is easy to show that $d + e\{0, 1, -1\} = f + g\{0, 1, -1\}$ if and only if $d = f$ and $e = -g$. If $3 = 0$, $d + e\{0, 1, -1\} = f + g\{0, 1, -1\}$ if and only if one of the following five situations occurs:

1) $d = f$ and $e = -g$,,
2) $d = f + g$ and $e = g$,
3) $d = f + g$ and $e = -g$,
4) $d = f - g$ and $e = g$,
5) $d = f - g$ and $e = -g$.

Therefore, the conclusion follows. ◆

Lemma 3.3.5 $|\langle 1, \mu, \mu^2\rangle| = q(q - 1) / 3$, where $\mu^3 = 1$.

Proof. Note $\mu^3 = 1$ implies that $q \equiv 1 \pmod 6$. Suppose $(d, e) \neq (f, g)$, $d, f \in F_q$ and $e, g \in F_q^*$. We want to know when $d + e\{1, \mu, \mu^2\} = f + g\{1, \mu, \mu^2\}$.

$d + e\{1, \mu, \mu^2\} = f + g\{1, \mu, \mu^2\}$ holds if and only if one of the following six relations is satisfied.

(1)	$d + e = f + g$;	$d + e\mu = f + g\mu$;	$d + e\mu^2 = f + g\mu^2$
(2)	$d + e = f + g$;	$d + e\mu = f + g\mu^2$;	$d + e\mu^2 = f + g\mu$
(3)	$d + e = f + g\mu$;	$d + e\mu = f + g$;	$d + e\mu^2 = f + g\mu^2$
(4)	$d + e = f + g\mu$;	$d + e\mu = f + g\mu^2$;	$d + e\mu^2 = f + g$
(5)	$d + e = f + g\mu^2$;	$d + e\mu = f + g$;	$d + e\mu^2 = f + g\mu$
(6)	$d + e = f + g\mu^2$;	$d + e\mu = f + g\mu$;	$d + e\mu^2 = f + g$

From (1), we have $(d, e) = (f, g)$, a contradiction. (2) yields a contradiction like $(1 + \mu)^2 = 0$. It is the same in cases (3) and (6). (4) will produce $d = f$ and $e = \mu g$. (5) will produce $d = f$ and $e = \mu^2 g$. Therefore, $|\langle 1, \mu, \mu^2\rangle| = q(q - 1) / 3$. ◆

Lemma 3.3.6 $|\langle A\rangle| = q(q - 1)$ if the following are satisfied:

1) $A \notin \langle 0, 1, -1\rangle$,
2) $A \notin \langle 1, \mu, \mu^2\rangle$ provided $\mu^3 = 1$.

Proof. Let $A = \{a, b, c\}$. Suppose $(d, e) \neq (f, g)$, $d, f \in F_q$ and $e, g \in F_q^*$. We investigate when $d + eA = f + gA$ happens.

It happens when one of the following six relations holds.

(1) $d + ea = f + ga$; $d + eb = f + gb$; $d + ec = f + gc$
(2) $d + ea = f + ga$; $d + eb = f + gc$; $d + ec = f + gb$
(3) $d + ea = f + gb$; $d + eb = f + ga$; $d + ec = f + gc$
(4) $d + ea = f + gb$; $d + eb = f + gc$; $d + ec = f + ga$
(5) $d + ea = f + gc$; $d + eb = f + ga$; $d + ec = f + gb$
(6) $d + ea = f + gc$; $d + eb = f + gb$; $d + ec = f + ga$

Case (1) will give $a = b = c$, a contradiction, since A is a triple. (2) will produce $2a = b + c$, that is, $(0, b - a, c - a) \sim (0, 1, -1)$. Since $(a, b, c) \sim (0, b - a, c - a)$, $A \sim \{0, 1, -1\}$; that is a contradiction. (3) and (6) will yield $2c = a + b$ and $2b = a + c$ respectively. In the same way, (3) and (6) can not hold.

Now we consider case (4). Let $\eta = e / g$, $t = (f - d) / g$. The the equations in (4) become

$$\eta a = t + b; \qquad \eta b = t + c; \qquad \eta c = t + a.$$

Thus

$$\eta(a - b) = b - c; \qquad \eta(b - c) = c - a; \qquad \eta(c - a) = a - b.$$

Since $a \neq b \neq c \neq a$, the above will produce $\eta^3 = 1$. Since $\eta(c - a) = a - b$, $(c - a) / (b - a) = -\eta^2$. Hence $\{a, b, c\} \sim \{0, b - a, c - a\} \sim \{0, 1, (c - a) / (b - a)\} \sim \{0, 1, -\eta^2\} \sim \{0, 1, 1 + \eta\} \sim \{0, \eta - 1, \eta^2 - 1\} \sim \{1, \eta, \eta^2\}$, a contradiction. In the same way, (5) is not possible.

Therefore, if $(d, e) \neq (f, g)$, then $d + eA \neq f + gA$. Then the conclusion follows. ◆

Now we know that $\mathcal{P}_3(F_q)$ can be partitioned into equivalence classes. Among them, there is one and only one class $\langle 0, 1, -1 \rangle$ of size $q(q - 1) / 2$. If $q \equiv 1 \pmod 6$, there is one and only one class $\langle 1, \mu, \mu^2 \rangle$ of size $q(q - 1) / 3$, where $\mu^3 = 1$. All the other classes are of size $q(q - 1)$.

For $A \in \mathcal{P}_3(F_q)$, define $dev_p A$ to be the set consisting of $d + A$ ($d \in F_q$). If $\mathcal{A} \subseteq \mathcal{P}_3(F_q)$, define $dev_p \mathcal{A} = \cup_{A \in \mathcal{A}} dev_p A$. Obviously $<A> = dev_p \mathcal{A}$, where $\mathcal{A} = \{eA : e \in F_q^*\}$. For $A \in \mathcal{P}_3(F_q)$, $|dev_p A| = q$.

Lemma 3.3.7 Suppose $A, B \in <0, 1, -1>$. If $A = -B$, then $dev_p A = dev_p B$. If $A = eB$, but $e \notin \{1, -1\}$, then $dev_p A \cap dev_p B = \emptyset$.

Proof. If $A = -B$, since $A, B \in <0, 1, -1>$, then it is easy to show that $B \in dev_p A$. Therefore, $dev_p A = dev_p B$. We know that $<0, 1, -1> = \cup_{e \in Fp^*} dev_p e\{0, 1, -1\}$. Since $|<0, 1, -1>| = q(q-1)/2$, $dev_p A \cap dev_p B = \emptyset$ must hold if $A = eB$, $e \notin \{1, -1\}$. ♦

Lemma 3.3.8 Suppose $A, B \in <1, \mu, \mu^2>$, where $\mu^3 = 1$. If $A = \mu B$ or $A = \mu^2 B$, then $dev_p A = dev_p B$. If $A = eB$, but $e \notin \{1, \mu, \mu^2\}$, then $dev_p A \cap dev_p B = \emptyset$.

Proof. The process is similar to that of Lemma 3.3.7. ♦

Lemma 3.3.9 Suppose $A, B \in \mathcal{P}_3(F_q)$, $A, B \notin <0, 1, -1>$ and $A, B \notin <1, \mu, \mu^2>$, if $\mu^3 = 1$. If $A = eB$, but $e \neq 1$, then $dev_p A \cap dev_p B = \emptyset$.

Proof. Since $|<A>| = q(q-1)$ and $<A> = dev_p \mathcal{A}$, where $\mathcal{A} = \{eA : e \in F_q^*\}$, $dev_p A \cap dev_p B = \emptyset$ must hold if $A = eB$, but $e \neq 1$. ♦

$\mathcal{P}_3(F_q)$ is divisible into equivalence classes using the equivalence relation ~. A *representative* of a class is just a member of that class. Let $\mathcal{R}$ be a set of representatives of all equivalence classes. $\mathcal{R}$ is called a *representative set* of $\mathcal{P}_3(F_q)$. Of course, $\mathcal{R}$ is not unique, since a representative of a class is not unique.

Now we focus on the finite field Z_p. We try to construct a STS(p+2), from which we try to get a large set LS(p+2). Let the point set be

$$X = \{\infty_1, \infty_2\} \cup Z_p.$$

Suppose ξ is a primitive element in Z_p. For $\alpha \in \{\infty_1, \infty_2\}$, $i \in Z_p$, define $i\alpha = \alpha$ and $\alpha + i = \alpha$. To construct a GLS(p+2), we construct the first STS(p+2) $\mathcal{A}_0$, from which the others can be developed, i.e., define

$$\mathcal{A}_i = \{i + A : A \in \mathcal{A}_0\}$$

such that $\mathcal{A}_i$ $(0 \le i \le p - 1)$ will form a GLS(p+2). In order to narrow down the search, we require that $\mathcal{A}_0$ satisfy the following conditions.

(3.3.1) $\{\infty_1, \infty_2, 0\} \in \mathcal{A}_0$.

(3.3.2) $\xi^{2hi}\{\infty_1, \xi^j, \xi^{h+j}\} \in \mathcal{A}_0$,
$\xi^{2hi}\{\infty_2, \xi^{h+j}, \xi^{2h+j}\} \in \mathcal{A}_0$,
$0 \le i \le m - 1, 0 \le j \le h - 1$, where $h = 2^{k-1}$ if $p - 1 = 2^k m$ and $m > 1$ is odd.

(3.3.3) $eR \in \mathcal{A}_0$, $e \in Z_p^*$, $R \in \mathcal{R}$, where $\mathcal{R}$ is a representative set of $\mathcal{P}_3(Z_p)$.

From the above construction scheme, to construct $\mathcal{A}_0$ we just need to find the proper $\mathcal{R}$. To further restrict ourselves, let $\{0, 1, - 1\} \in \mathcal{R}$. If $p \equiv 1 \pmod 6$, let $\{1, \mu, \mu^2\} \in \mathcal{R}$, where $\mu = \xi^{(p-1)/3}$. Since $\mathcal{A}_0$ can not have repeated blocks, we let $\xi^i\{0, 1, - 1\} \in \mathcal{A}_0$ only if $0 \le i < (p - 1) / 2$; let $\xi^i\{1, \mu, \mu^2\} \in \mathcal{A}_0$ only if $0 \le i < (p - 1) / 3$.

Once we have $\mathcal{R}$, how can we check that the $\mathcal{A}_0$ obtained is an STS(p+2)? We mainly check *exponential differences* which are defined as follows. The triple $\{\xi^i, \xi^j, \xi^k\}$ has exponential differences

$$\pm (i - j) \pmod{p - 1}, \pm (i - k) \pmod{p - 1}, \pm (j - k) \pmod{p - 1}.$$

If $p \equiv 1 \pmod 6$, $\{1, \xi^{(p-1)/3}, \xi^{(p-1)2/3}\}$ has one exponential difference

$$\pm (p - 1) / 3 \pmod{p - 1}.$$

$\{0, \xi^i, \xi^j\}$ has exponential differences

$$\pm(i - j) \pmod{p - 1}.$$

To ensure that $\mathcal{A}_0$ be a STS(p+2), we assume $\mathcal{R}$ satisfies the following:

(3.3.4) $\mathcal{R}$ produces exponential difference $i \in Z_p \setminus \{0, h\}$ exactly once.

Property of $\mathcal{R}$ ensures that $\mathcal{A}_i$ $(0 \le i \le p - 1)$ are mutually disjoint.

Finally, we mention that LS(p+2) developed from $\mathcal{A}_0$ is a GLS(p+2). The reason is the following. If we define

$$D(\mathcal{A}_i, \infty_1, \infty_2) = \{(i + \xi^j, i + \xi^{h+j}): 0 \le j \le p - 2\},$$

then $D(\mathcal{A}_i, \infty_1, \infty_2) \cap D(\mathcal{A}_{i'}, \infty_1, \infty_2) = \varnothing$, $i \neq i'$.

In Appendix I, we present $\mathcal{R}$. Therefore, we have the following.

Lemma 3.3.10 Suppose prime number $p \equiv 1 \pmod 8$ and $p \le 137$. Then there exists a GLS(p+2).

Lemma 3.3.11 Suppose prime number $p \equiv 1 \pmod 8$ and $p \le 137$. Suppose an LSDG(t^{u+2}) exists. Then an LSDG(t^{up+2}) exists.

Proof. By Lemma 3.3.10 and Lemma 3.2.2. ♦

We remark here that the construction outlined above does not work for $p \equiv 5 \pmod 8$. The argument is as follows. For $R \in \mathcal{R}$, the six exponential differences produced by R will be either (1) all even or (2) two even and four odd. From this fact, it is not difficult to conclude that it is impossible to make $\mathcal{R}$satisfy (3.3.4) if $p \equiv 5 \pmod 8$.

The spectrum of GLS(v) remains largely undetermined. Therefore, in the next section we give a construction that does not need a GLS(v).

3.4 Construction II

In this section, we give a recursive construction for LSDG(t^u), where t even. We need some special classes of LSDG($2^{u+1}(2u)^1$), which we describe now.

Suppose ∞, ∞', a and b are four distinct symbols, and $k \in Z_{2u}$. Let $w = \lceil \frac{u}{2} \rceil$. Define $\mathcal{C}(\infty, \infty', a, b; k)$ to be the following set of blocks, developed modulo 2u:

$\{\infty, (a, 0), (b, k)\}$,
$\{\infty', (a, -w), (b, k)\}$,

$\{(a, i), (a, -i), (b, k)\}$ for $1 \le i \le w - 1$,

$\{(a, i), (a, -i - 1), (b, k)\}$ for $w \le i \le u - 1 \pmod{2u}$.

Suppose we take a set of points

$$X = \{\infty, \infty'\} \cup (\{a, b\} \times Z_{2u})$$

and let $\mathcal{G}$ consist of the following groups:

$$\{\infty, \infty'\}, \{(a, i), (a, i + u)\} \ (0 \le i \le u - 1) \text{ and } \{b\} \times Z_{2u}.$$

Then $(X, \mathcal{G}, \mathcal{C}(\infty, \infty', a, b; k))$ is a 3-GDD$(2^{u+1}(2u)^1)$. If we let k run over Z_{2u}, we get an LSDG$(2^{u+1}(2u)^1)$.

The following property will be important for our construction.

Lemma 3.4.1 Suppose $\{\alpha, \beta, \gamma, \delta\} \cap \{a, b, c, d\} = \varnothing$, and let $j, k \in Z_{2u}$. Then $\mathcal{C}(\alpha, \beta, a, b; j) \cap \mathcal{C}(\gamma, \delta, c, d; k) = \varnothing$ if any of the following is satisfied:

1) $\{a, b\} \neq \{c, d\}$,
2) $(a, b) = (c, d)$ and $j \neq k$,
3) $(a, b) = (d, c)$, $\{\alpha, \beta\} \cap \{\gamma, \delta\} = \varnothing$,
4) $(a, b) = (d, c)$, $(\alpha, \beta) = (\delta, \gamma)$ and $j + k \not\equiv -w \pmod{2u}$, where $w = \lceil \frac{u}{2} \rceil$.

Next we prove a simple numerical lemma.

Lemma 3.4.2 Let u be a positive integer and let $w = \lceil \frac{u}{2} \rceil$.

1) If w is odd (i.e., $u \equiv 1$ or $2 \pmod 4$), then there exist subsets N_0 and N_1 of Z_{2u} such that $|N_0| = |N_1| = u$, $N_0 \cup N_1 = Z_{2u}$, and such that for $x, y \in N_i$ $(i = 0 \text{ or } 1)$, $x + y \not\equiv -w \pmod{2u}$.
2) If w is even, (i.e., $u \equiv 0$ or $3 \pmod 4$), then there exist subsets N_0 and N_1 of Z_{2u} such that $|N_0| = |N_1| = u$, $N_0 \cup N_1 = Z_{2u}$, and such that for $x \in N_0$, $y \in N_1$, $x + y \not\equiv -w \pmod{2u}$.

Proof. First assume w is odd. Then there are u pairs $\{x, y\}$ in Z_{2u} with $x + y \equiv - w \pmod{2u}$ and $x \neq y$. For each such pair, place one element in N_0 and the other in N_1.

Next assume w is even. There are u - 1 pairs $\{x, y\}$ with $x + y \equiv - w \pmod{2u}$ and $x \neq y$. Also, there are two elements satisfying $2x \equiv - w \pmod{2u}$, namely, $2u - w / 2$ and $u - w / 2$. If u is odd, then let N_0 consist of $(u - 1) / 2$ of the pairs and one of the two special elements, and let $N_1 = Z_{2u} \setminus N_0$. If u is even, then let N_0 consist of $(u - 2) / 2$ of the pairs and both special elements, and let $N_1 = Z_{2u} \setminus N_0$. ♦

As in Section 3.2, we first show how to construct 2u disjoint 3-GDD($2^{u(v-2)+2}$) from an STS(v). Then, we construct an LSDG($2^{u(v-2)+2}$) from a LS(v), $v \equiv 1$ or 3 (mod 6), which need not be a GLS(v). The constructions are different in the cases w even and w odd (where $w = \lceil \frac{u}{2} \rceil$).

First we consider the case w odd. Let $v \equiv 1$ or 3 (mod 6), and let $(X, \mathcal{A})$ be an STS(v) on point set $X = \{\infty, \infty'\} \cup Z_{v-2}$. Define $E(\mathcal{A}, \infty)$, $E(\mathcal{A}, \infty')$ and $D(\mathcal{A}, \infty, \infty')$ as in the proof of Lemma 3.2.1.

The point set for our 3-GDD($2^{u(v-2)+2}$) is

$$Y = (\{\infty, \infty'\} \times Z_2) \cup (Z_{v-2} \times Z_{2u})$$

and the group set $\mathcal{G}$ consists of

$$\{\infty\} \times Z_2, \{\infty'\} \times Z_2, \text{ and } \{i\} \times \{j, j + u\} \ (i \in Z_{v-2}, 0 \leq j \leq u - 1).$$

The block sets are constructed as follows.

Construct N_0 and N_1 as in Lemma 3.4.2. Then for each $A \in \mathcal{A}$, do the following.

1) If $A = \{a, b, c\}$, $a, b, c \in Z_{v-2}$, then take an LSDG($(2u)^3$) on point set $A \times Z_{2u}$, with groups $\{a\} \times Z_{2u}$, $\{b\} \times Z_{2u}$, and $\{c\} \times Z_{2u}$. Name the 2u block sets $\mathcal{B}(A, j)$, $j \in Z_{2u}$.

2) If $A = \{\infty, a, b\}$ and $(a, b) \in D(\mathcal{A}, \infty, \infty')$, take the 2u sets of blocks $\mathcal{C}((\infty, 0), (\infty, 1), a, b; j)$, $j \in N_0$; and $\mathcal{C}((\infty, 1), (\infty, 0), b, a; j)$, $j \in N_0$. Rename them $\mathcal{B}(A, j)$, $j \in Z_{2u}$, in such a way that $\{\mathcal{B}(A, j), j \in N_0\} = \{\mathcal{C}((\infty, 0), (\infty, 1), a, b; j): j \in N_0\}$.

3) If $A = \{\infty', a, b\}$ and $(a, b) \in D(\mathcal{A}, \infty, \infty')$, take the 2u sets of blocks $\mathcal{C}((\infty', 0), (\infty', 1), a, b; j)$, $j \in N_1$; and $\mathcal{C}((\infty', 1), (\infty', 0), b, a; j)$, $j \in N_1$. Rename them $\mathcal{B}(A, j)$, $j \in Z_{2u}$, in such a way that $\{\mathcal{B}(A, j), j \in N_0\} = \{\mathcal{C}((\infty, 0), (\infty, 1), a, b; j): j \in N_1\}$.

4) If $A = \{\infty, \infty', z\}$, then take an LSDG($t^{u+2}$) on point set $(\{\infty, \infty'\} \times Z_2) \cup (\{z\} \times Z_{2u})$, with groups $\{\infty\} \times Z_2$, $\{\infty'\} \times Z_2$, $\{(z, j), (z, u + j)\}$ $(0 \le j \le u - 1)$. Rename the block sets $\mathcal{B}(A, j)$, $j \in Z_{2u}$.

For any $j \in Z_{2u}$, define

$$\mathcal{B}(j) = \bigcup_{A \in \mathcal{A}} \mathcal{B}(A, j).$$

Then each $(Y, \mathcal{G}, \mathcal{B}(j))$ is a 3-GDD($2^{u(v-2)+2}$). These 3-GDD are disjoint as can be verified using Lemma 3.4.1 and 3.3.2. The only "tricky" part is the following. If there were $j, j' \in N_i$, with $j + j' \equiv -w \pmod{2u}$ $(i = 0 \text{ or } 1)$, then $\mathcal{C}((\alpha, 0), (\alpha, 1), a, b; j) \cap \mathcal{C}((\alpha, 1), (\alpha, 0), b, a; j') \neq \emptyset$, $(\alpha = \infty \text{ or } \infty')$. However, this is ruled out by the method of construction of N_0 and N_1 in Lemma 3.4.2.

If we start with an LS(v), $v \equiv 1$ or $3 \pmod 6$, and carry out the above construction for each STS(v) in it, we will obtain an LSDG($2^{u(v-2)+2}$).

Lemma 3.4.3 Suppose there is an LS(v), $v \equiv 1$ or $3 \pmod 6$. If there exists an LSDG(2^{2+u}), then there is an LSDG($2^{u(v-2)+2}$).

Proof. The verification is straightforward, using Lemma 3.4.1 and 3.4.2. ♦

We now turn to the case when $w = \lceil \frac{u}{2} \rceil$ is even. We start with an STS(v), $(X, \mathcal{A})$, and define Y and $\mathcal{G}$ as in the case w odd. Define $E(\mathcal{A}, \infty)$, $E(\mathcal{A}, \infty')$ and $D(\mathcal{A}, \infty, \infty')$ as before. Construct N_0 and N_1 according to Lemma 3.4.2 (this part is different from the case w odd).

Next let $\Psi: E(\mathcal{A}, \infty) \cup E(\mathcal{A}, \infty') \to \{N_0, N_1\}$ be any function. For $A \in \mathcal{A}$, construct the following sets of blocks.

1) If $A = \{a, b, c\}$, $a, b, c \in Z_{v-2}$, then $\mathcal{B}(A, j)$, $j \in Z_{2u}$, are constructed as in the case w odd.

2) If $A = \{\infty, a, b\}$ and $(a, b) \in D(\mathcal{A}, \infty, \infty')$, take the 2u sets of blocks $\mathcal{C}((\infty, 0), (\infty, 1), a, b; j)$, $j \in \Psi(a, b)$; and $\mathcal{C}((\infty, 1), (\infty, 0), b, a; j)$, $j \notin \Psi(a, b)$. Rename them $\mathcal{B}(A, j)$, $j \in Z_{2u}$, in such a way that $\{\mathcal{B}(A, j), j \in N_0\} = \{\mathcal{C}((\infty, 0), (\infty, 1), a, b; j): j \in \Psi(a, b)\}$.

3) If $A = \{\infty', a, b\}$ and $(a, b) \in D(\mathcal{A}, \infty, \infty')$, take the 2u sets of blocks $\mathcal{C}((\infty', 0), (\infty', 1), a, b; j)$, $j \in \Psi(a, b)$; and $\mathcal{C}((\infty', 1), (\infty', 0), b, a; j)$, $j \notin \Psi(a, b)$. Rename them $\mathcal{B}(A, j)$, $j \in Z_{2u}$, in such a way that $\{\mathcal{B}(A, j), j \in N_0\} = \{\mathcal{C}((\infty', 0), (\infty', 1), a, b; j): j \in \Psi(a, b)\}$.

4) If $A = \{\infty, \infty', z\}$, then $\mathcal{B}(A, j)$, $j \in Z_{2u}$, are constructed as in the case w odd.

For any $j \in Z_{2u}$, define

$$\mathcal{B}(j) = \bigcup_{A \in \mathcal{A}} \mathcal{B}(A, j).$$

Again we have 2u disjoint 3-GDD$(2^{u(v-2)+2})$s. The difference between the cases w even and w odd is in the blocks of type 2 and 3. As before, we need to ensure that we have not included two sets $\mathcal{C}((\alpha, 0), (\alpha, 1), a, b; j)$ and $\mathcal{C}((\alpha, 1), (\alpha, 0), b, a; j')$, with $j + j' \equiv -w \pmod{2u}$, ($\alpha = \infty$ or ∞'). This is ensured by the fact that one of j and j' is in N_0 and the other in N_1.

When we start with an LS(v), $v \equiv 1$ or $3 \pmod 6$, we can obtain an LSDG$(2^{u(v-2)+2})$ if we define Ψ properly for each STS(v). For each of the v - 2 STS(v)s, say $(X, \mathcal{A}_i)$ $(1 \le i \le v - 2)$, we define a different Ψ_i: $E(\mathcal{A}_i, \infty) \cup E(\mathcal{A}_i, \infty') \to \{N_0, N_1\}$. We want a certain property to be satisfied for every unordered pair $\{a, b\}$, which is described as follows.

Suppose $\{a, b\} \in E(\mathcal{A}_i, \infty) \cap E(\mathcal{A}_{i'}, \infty')$ (this determines i and i' uniquely). We require the following property.

(3.4.1) $\Psi_i\{a, b\} = \Psi_{i'}\{a, b\}$ if and only if $\{a, b\}$ is directed differently in $D(\mathcal{A}_i, \infty, \infty')$ and $D(\mathcal{A}_{i'}, \infty, \infty')$.

It is easy to construct the mappings Ψ_i $(1 \le i \le v - 2)$ so that (3.4.1) is satisfied. They can be defined by the following algorithm.

FOR i = 1 TO v - 2 DO
FOR each pair $\{a, b\} \in E(\mathcal{A}_i, \infty) \cup E(\mathcal{A}_i, \infty')$ DO
IF there exists $i' < i$ so that $\{a, b\} \in E(\mathcal{A}_{i'}, \infty) \cup E(\mathcal{A}_{i'}, \infty')$ THEN
define $\Psi_i(a, b)$ so that (3.4.1) is satisfied
ELSE
define $\Psi_i(a, b) = N_0$ or N_1 arbitrarily.

Then we have the following.

Lemma 3.4.4 Suppose there is an LS(v), $v \equiv 1$ or 3 (mod 6). If there is an LSDG(2^{u+2}), then there is an LSDG($2^{u(v-2)+2}$).

Proof. Define the mapping Ψ_i ($1 \le i \le v - 2$) as described above, and construct 2u 3-GDD($2^{u(v-2)+2}$) from each STS(v). The resulting set of 3-GDDs can be seen to be disjoint. The mappings Ψ_i are required for the following reason. Suppose $\{a, b\} \in E(\mathcal{A}_i, \infty) \cap E(\mathcal{A}_{i'}, \infty')$. If $(a, b) \in D(\mathcal{A}_i, \infty, \infty') \cap D(\mathcal{A}_{i'}, \infty, \infty')$, then we have the following four sets of blocks:

1) $\mathcal{C}((\infty, 0), (\infty, 1), a, b; j)$, $j \in \Psi_i(a, b)$,
2) $\mathcal{C}((\infty, 1), (\infty, 0), b, a; j)$, $j \notin \Psi_i(a, b)$,
3) $\mathcal{C}((\infty', 0), (\infty', 1), a, b; j)$, $j \in \Psi_{i'}(a, b)$,
4) $\mathcal{C}((\infty', 1), (\infty', 0), b, a; j)$, $j \notin \Psi_{i'}(a, b)$.

In order that the sets 1 and 3 be disjoint, we need $\Psi_i(a, b) \neq \Psi_{i'}(a, b)$. Then, sets 2 and 4 are disjoint as well. A similar argument applies if $\{a, b\}$ is directed differently in $D(\mathcal{A}_i, \infty, \infty')$ and $D(\mathcal{A}_{i'}, \infty, \infty')$. ♦

The above lemma can not be applied with v = 7, since LS(7) does not exist. However, a modified construction will work.

Lemma 3.4.5 If there is an LSDG(2^{u+2}), then there is an LSDG(2^{5u+2}).

Proof. Suppose N_0 and N_1 are abtained in Z_{2u}. Define $w = \lceil \frac{u}{2} \rceil$. We will construct an LSDG(2^{5u+2}) with the point set

$$Y = (\{\infty, \infty'\} \times Z_2) \cup (Z_5 \times Z_{2u})$$

and the group set $\mathcal{G}$ consisting of

$$\{\infty\} \times Z_2,\ \{\infty'\} \times Z_2, \text{ and } \{(i, j), (i, j + u)\},\ (i \in Z_5,\ 0 \le j \le u - 1).$$

First we construct the following set of blocks.

1) For each $i \in Z_5$, take an LSDG(2^{u+2}), on points $(\{\infty, \infty'\} \times Z_2) \cup (\{i\} \times Z_{2u})$, with groups $\{\infty\} \times Z_2$, $\{\infty'\} \times Z_2$, and $\{(i, j), (i, j + u)\}$ $(0 \le j \le u - 1)$. Denote the block sets by $\mathcal{B}_1(i, j)$, $j \in Z_{2u}$.

2) For each $i \in Z_5$, take an LSDG($(2u)^3$), on points $\{i, i + 1, i + 4\} \times Z_{2u}$, with groups $\{i\} \times Z_{2u}$, $\{i + 1\} \times Z_{2u}$, $\{i + 4\} \times Z_{2u}$. Denote the block sets by $\mathcal{B}_2(i, j)$, $j \in Z_{2u}$.

3) For each $i \in Z_5$, take an LSDG($(2u)^3$), on points $\{i, i + 2, i + 3\} \times Z_{2u}$, with groups $\{i\} \times Z_{2u}$, $\{i + 2\} \times Z_{2u}$, $\{i + 3\} \times Z_{2u}$. Denote the block sets by $\mathcal{B}_3(i, j)$, $j \in Z_{2u}$.

4) There are two cases according as w is even or odd. If w is odd, then define

$$\mathcal{C}_1(i, j) = \mathcal{C}((\infty, 0), (\infty, 1), i + 1, i + 3; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_2(i, j) = \mathcal{C}((\infty, 1), (\infty, 0), i + 4, i + 2; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_3(i, j) = \mathcal{C}((\infty, 0), (\infty, 1), i + 3, i + 4; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_4(i, j) = \mathcal{C}((\infty, 1), (\infty, 0), i + 2, i + 1; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_5(i, j) = \mathcal{C}((\infty', 0), (\infty', 1), i + 3, i + 4; j)\ i \in Z_5, j \in N_1;$$
$$\mathcal{C}_6(i, j) = \mathcal{C}((\infty', 1), (\infty', 0), i + 2, i + 1; j)\ i \in Z_5, j \in N_1;$$
$$\mathcal{C}_7(i, j) = \mathcal{C}((\infty', 0), (\infty', 1), i + 4, i + 2; j)\ i \in Z_5, j \in N_1;$$
$$\mathcal{C}_8(i, j) = \mathcal{C}((\infty', 1), (\infty', 0), i + 1, i + 3; j)\ i \in Z_5, j \in N_1.$$

If w is even, define

$$\mathcal{C}_1(i, j) = \mathcal{C}((\infty, 0), (\infty, 1), i + 1, i + 3; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_2(i, j) = \mathcal{C}((\infty, 1), (\infty, 0), i + 4, i + 2; j)\ i \in Z_5, j \in N_1;$$
$$\mathcal{C}_3(i, j) = \mathcal{C}((\infty, 0), (\infty, 1), i + 3, i + 4; j)\ i \in Z_5, j \in N_1;$$
$$\mathcal{C}_4(i, j) = \mathcal{C}((\infty, 1), (\infty, 0), i + 2, i + 1; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_5(i, j) = \mathcal{C}((\infty', 0), (\infty', 1), i + 3, i + 4; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_6(i, j) = \mathcal{C}((\infty', 1), (\infty', 0), i + 2, i + 1; j)\ i \in Z_5, j \in N_1;$$

$$\mathcal{C}_7(i, j) = \mathcal{C}((\infty', 0), (\infty', 1), i + 4, i + 2; j)\ i \in Z_5, j \in N_0;$$
$$\mathcal{C}_8(i, j) = \mathcal{C}((\infty', 1), (\infty', 0), i + 1, i + 3; j)\ i \in Z_5, j \in N_1.$$

Observe that all the blocks in (1) - (4) are distinct by Lemma 3.4.1. We now show the construction of LSDG(2^{5u+2}) from these block sets. First define a 1-1 mapping η: $Z_{2u} \rightarrow Z_{2u}$ such that $\{\eta(j): 0 \le j \le u - 1\} = N_0$ (hence $\{\eta(j): u \le j \le 2u - 1\} = N_1$).

There are two cases.

If w is odd, define the following sets of blocks

1) For $i \in Z_5$, $0 \le j \le u - 1$, let $\mathcal{B}(i, j) = \mathcal{B}_1(i, j) \cup \mathcal{B}_2(i, j) \cup \mathcal{B}_3(i, j) \cup \mathcal{C}_1(i, \eta(j)) \cup \mathcal{C}_1(i, \eta(j)) \cup \mathcal{C}_5(i, \eta(j + u)) \cup \mathcal{C}_6(i, \eta(j + u))$.
2) For $i \in Z_5$, $u \le j \le 2u - 1$, let $\mathcal{B}(i, j) = \mathcal{B}_1(i, j) \cup \mathcal{B}_2(i, j) \cup \mathcal{B}_3(i, j) \cup \mathcal{C}_3(i, \eta(j - u)) \cup \mathcal{C}_4(i, \eta(j - u)) \cup \mathcal{C}_7(i, \eta(j)) \cup \mathcal{C}_8(i, \eta(j))$.

If w is even, define the following sets of blocks

1) For $i \in Z_5$, $0 \le j \le u - 1$, let $\mathcal{B}(i, j) = \mathcal{B}_1(i, j) \cup \mathcal{B}_2(i, j) \cup \mathcal{B}_3(i, j) \cup \mathcal{C}_1(i, \eta(j)) \cup \mathcal{C}_1(i, \eta(j + u)) \cup \mathcal{C}_5(i, \eta(j)) \cup \mathcal{C}_6(i, \eta(j + u))$.
2) For $i \in Z_5$, $u \le j \le 2u - 1$, let $\mathcal{B}(i, j) = \mathcal{B}_1(i, j) \cup \mathcal{B}_2(i, j) \cup \mathcal{B}_3(i, j) \cup \mathcal{C}_3(i, \eta(j)) \cup \mathcal{C}_4(i, \eta(j - u)) \cup \mathcal{C}_7(i, \eta(j - u)) \cup \mathcal{C}_8(i, \eta(j))$.

Then each $\mathcal{B}(i, j)$ is the block set of a 3-GDD(2^{5u+2}). Therefore, we have an LSDG(2^{5u+2}). ♦

For $v \equiv 1$ or 3 (mod 6), $v > 7$, there exists an LS(v) ([20], [21] and [30]). We combine Lemma 3.4.3, 3.4.4 and 3.4.5 as follows.

Lemma 3.4.6 Suppose there exists an LSDG(2\s(u+2)). Then there exists an LSDG($2^{u(v-2)+2}$), where $v \equiv 1$ or 3 (mod 6), $v > 1$.

We can generalize the previous constructions to even values of t other than 2. Suppose $t = 2s$ and let u be an integer, and $w = \lceil \frac{u}{2} \rceil$. Then given distinct symbols ∞, ∞', a and b, any $k \in$

Z_{2u}, define $\mathcal{C}(\infty, \infty', a, b; k)$ as before. Recall that $(X, \mathcal{G}, \mathcal{C}(\infty, \infty', a, b; k))$ is a 3-GDD$(2^{u+1}(2u)^1)$, on point set

$$X = \{\infty, \infty'\} \cup (\{a, b\} \times Z_{2u}),$$

having group set $\mathcal{G}$ consisting of

$$\{\infty, \infty'\}, \{(a, i), (a, i + u)\} \ (0 \le i \le u - 1), \text{ and } \{b\} \times Z_{2u}.$$

Define some arbitrary ordering on the points in X. Now, for any $y \in Z_s$, we construct a set of blocks $\mathcal{D}(\infty, \infty', a, b; k, y)$ with $x_1 < x_2 < x_3$. Take the s^2 blocks $\{(x_1, s_1), (x_2, s_2), (x_3, s_3)\}$ where $s_1 + s_2 + s_3 \equiv y \pmod s$. For each group $G \in \mathcal{G}$, take a new group $G \times Z_s$, and obtain a 3-GDD$(t^{u+1}(tu)^1)$. Further, if we let k vary over Z_{2u} and y vary over Z_s, we get a set of $2us = tu$ disjoint 3-GDDs, i.e., a large set.

The constructions in Lemma 3.4.3 and 3.4.4 can now be adapted in an obvious way to handle any even t: wherever a set of blocks $\mathcal{C}(\infty, \infty', a, b; k)$ was used, we now take the s sets of blocks $\mathcal{D}(\infty, \infty', a, b; k, y)$, $y \in Z_s$.

We obtain the following result.

Lemma 3.4.7 Suppose $v \equiv 1$ or 3 (mod 6), $v > 1$, and there exists an LSDG(t^{u+2}), where t is even. Then there exists an LSDG$(t^{u(v-2)+2})$.

3.5 Construction III (using prime $p \equiv 5 \bmod 8$)

The construction in section 3.2 needs GLS(v), whose spectrum has not been decided yet. The construction in section 3.4 only works for GDD with even group size. In this section we try to throw away these requirements and restrictions. For some $v = p + 2$, where prime $p \equiv 5 \pmod 8$, we can do so.

Suppose an LSDG(t^{u+2}) exists. If t is even and p prime, an LSDG(t^{up+2}) exists by Lemma 3.4.7. So, we only consider t odd in this section. t odd implies that u is odd.

Suppose ∞, a and b are three distinct symbols. Suppose u is odd. For $i \in Z_u$, $j \in Z_t$, we construct a 3-GDD($t^{u+1}(tu)^1$) on point set

$$Y = (\{\infty\} \cup (\{a\} \times Z_u) \cup (\{b\} \times Z_u)) \times Z_t,$$

with groups

$$\{\infty\} \times Z_t,\ \{a\} \times \{k\} \times Z_t\ (k \in Z_u),\ \text{and}\ \{b\} \times Z_u \times Z_t.$$

The block set, denoted by $(\infty, a, b)_(i, j)$, consists of the following blocks.

1) $\{(\infty, t_1), (a, u_1, t_2), (b, u_2, t_3)\}$, $u_1 - u_2 \equiv i \pmod u$, $t_1 + t_2 + t_3 \equiv j \pmod t$
2) $\{(a, u_1, t_1), (a, u_2, t_2), (b, u_3, t_3)\}$, $u_1 + u_2 - 2u_3 \equiv 2i \pmod u$, $t_1 + t_2 + t_3 \equiv j \pmod t$.

Lemma 3.5.1 Suppose $\{\alpha_1, \alpha_2\}$ and $\{a_1, a_2, b_1, b_2\}$ are disjoint, and $i_1, i_2 \in Z_u$, $j_1, j_2 \in Z_t$. Then $(\alpha_1, a_1, b_1)_(i_1, j_1) \cap (\alpha_2, a_2, b_2)_(i_2, j_2) = \varnothing$ if one of the following is satisfied:

1) $\{a_1, b_1\} \neq \{a_2, b_2\}$
2) $(a_1, b_1) = (a_2, b_2)$ and $(i_1, j_1) \neq (i_2, j_2)$
3) $(a_1, b_1) = (b_2, a_2)$ and $\alpha_1 \neq \alpha_2$
4) $(a_1, b_1) = (b_2, a_2)$, $\alpha_1 = \alpha_2$ and $i_1 \neq -i_2$.

Proof. The verification is straightforward. ♦

Suppose $p \equiv 5 \pmod 8$ is a prime. Given an LSDG(t^{u+2}), we now give a scheme to construct an LSDG(t^{up+2}).

Suppose ξ is a primitive element in Z_p. Since prime $p \equiv 5 \pmod 8$, 2 is a quadratic non-residue, i.e., $2 = \xi^h$ for an odd h, $0 < h < p - 1$. Suppose $X = \{\infty_1, \infty_2\} \cup Z_p$. We construct an STS(p+2) $(X, \mathcal{A})$ satisfying the following conditions.

(3.5.1) $\{\infty_1, \infty_2, 0\} \in \mathcal{A}$.

(3.5.2) The following triples are in $\mathcal{A}$:
$\{\infty_1, \xi^{4s}, \xi^{4s+h}\}$, $\{\infty_1, \xi^{4s+2}, \xi^{4s+2+h}\}$, where $0 \le s < (p - 1) / 4$,
$\{\infty_2, \xi^{4s+1}, \xi^{4s+1+h}\}$, $\{\infty_2, \xi^{4s+3}, \xi^{4s+3+h}\}$, where $0 \le s < (p - 1) / 4$,
$\{0, \xi^s, -\xi^s\}$, where $0 \le s < (p - 1) / 2$.

(3.5.3) $eR \in \mathcal{A}$, $e \in Z_p^*$, $R \in \mathcal{R}$, $R \notin \langle 0, 1, -1 \rangle$, where $\mathcal{R}$ is a representative set of $\mathcal{P}_3(Z_p)$.

In order to make $(X, \mathcal{A})$ a STS(p+2), we need $\mathcal{R}$ to satisfy the following condition.

(3.5.4) $\mathcal{R}$ produces exponential difference $i \in Z_p \setminus \{0, h\}$ exactly once.

If STS(p+2) $(X, \mathcal{A})$ is constructed as above, the following three variations of $(X, \mathcal{A})$ are STS(p+2) too. All of the variations are obtained by changing blocks in (3.5.2) of $(X, \mathcal{A})$, while keeping blocks in (3.5.1) and (3.5.3). They will be used in the proof of Lemma 3.5.2. The first variation changes (3.5.2) into

$$\begin{aligned}
&\{\infty_1, \xi^{4s}, \xi^{4s+h}\}, \{\infty_1, \xi^{4s+2}, \xi^{4s+2+h}\}, && \text{where } 0 \le s < (p-1)/4,\\
&\{\infty_2, \xi^{4s}, -\xi^{4s}\}, \{\infty_2, \xi^{4s+1}, -\xi^{4s+1}\}, && \text{where } 0 \le s < (p-1)/4,\\
&\{0, \xi^{4s+1}, \xi^{4s+1+h}\}, \{0, \xi^{4s+3}, \xi^{4s+3+h}\}, && \text{where } 0 \le s < (p-1)/4.
\end{aligned}$$

The second variation of $(X, \mathcal{A})$ changes (3.5.2) into

$$\begin{aligned}
&\{\infty_1, \xi^{4s}, -\xi^{4s}\}, \{\infty_1, \xi^{4s+1}, -\xi^{4s+1}\}, && \text{where } 0 \le s < (p-1)/4,\\
&\{\infty_2, \xi^{4s}, \xi^{4s+h}\}, \{\infty_2, \xi^{4s+2}, \xi^{4s+2+h}\}, && \text{where } 0 \le s < (p-1)/4,\\
&\{0, \xi^{4s+1}, \xi^{4s+1+h}\}, \{0, \xi^{4s+3}, \xi^{4s+3+h}\}, && \text{where } 0 \le s < (p-1)/4.
\end{aligned}$$

The third variation of $(X, \mathcal{A})$ changes (3.5.2) into

$$\begin{aligned}
&\{\infty_1, \xi^{4s+3}, \xi^{4s+3+h}\}, \{\infty_1, \xi^{4s+1}, \xi^{4s+1+h}\}, && \text{where } 0 \le s < (p-1)/4,\\
&\{\infty_2, \xi^{4s}, -\xi^{4s}\}, \{\infty_2, \xi^{4s+1}, -\xi^{4s+1}\}, && \text{where } 0 \le s < (p-1)/4,\\
&\{0, \xi^{4s}, \xi^{4s+h}\}, \{0, \xi^{4s+2}, \xi^{4s+2+h}\}, && \text{where } 0 \le s < (p-1)/4.
\end{aligned}$$

Since $\xi^h = 2$, $U(0, 1, -1) = U(0, 1, \xi^h)$. Thus, $\{0, \xi^{4s+1}, \xi^{4s+1+h}\}$, $\{0, \xi^{4s+3}, \xi^{4s+3+h}\}$, $\{0, \xi^{4s+1}, \xi^{4s+1+h}\}$, $\{0, \xi^{4s+3}, \xi^{4s+3+h}\}$, $\{0, \xi^{4s}, \xi^{4s+h}\}$, $\{0, \xi^{4s+2}, \xi^{4s+2+h}\}$ are all in $\langle 0, 1, -1 \rangle$, where $0 \le s < (p-1)/4$.

Note that, if we develop $\mathcal{A}$ mod p, we will not get an LS(p+2). The reason is

$$dev_p\{\{\infty_1, \xi^{4s}, \xi^{4s+h}\} : 0 \le s < (p-1)/4\}$$

and

$$dev_p\{\{\infty_1, \xi^{4s+2}, \xi^{4s+2+h}\} : 0 \le s < (p-1)/4\}$$

are not disjoint. But once we have constructed such an STS(p+2) (X, $\mathcal{A}$), we can use the following lemma.

Lemma 3.5.2 Suppose u is odd and $u \ge 5$. Suppose an LSDG(t^{u+2}) exists. If there is an STS(p+2) (X, $\mathcal{A}$) satisfying (3.5.1) -- (3.5.4), then there exists an LSDG(t^{up+2}).

Proof For {a, b, c} $\in \mathcal{A}$, where a,b,c $\in Z_p$, construct a GDD($(ut)^3$), with point set: {a, b, c} $\times Z_u \times Z_t$; with groups: {a} $\times Z_u \times Z_t$, {b} $\times Z_u \times Z_t$, {c} $\times Z_u \times Z_t$. The block set, denoted by (a, b, c)_(j, k), consists of the following triples: $\{(a,u_1,t_1), (b,u_2,t_2), (c,u_3,t_3)\}$, $u_1 + u_2 + u_3 \equiv j \pmod u$ and $t_1 + t_2 + t_3 \equiv k \pmod t$.

Let $S = \{eR : e \in Z_p^*,\ R \in \mathcal{R}, R \notin <0, 1, -1>\}$.

We now proceed to construct an LSDG(t^{up+2}). As point set, take

$$V = \{\infty_1,\infty_2\} \times Z_t \cup Z_p \times Z_u \times Z_t.$$

As group set, let $\mathcal{G}$ consist of

$$\{\infty_1\} \times Z_t,\ \{\infty_2\} \times Z_t,\ \{i\} \times \{j\} \times Z_t\ (i \in Z_p, j \in Z_u).$$

Define the following sets of blocks.

1) For each $i \in Z_p$, take an LSDG(t^{u+2}) on $\{\infty_1,\infty_2\} \times Z_t \cup \{i\} \times Z_u \times Z_t$. Name the ut block sets $\mathcal{A}_{ijk}$, $j \in Z_u$, $k \in Z_t$.
2) Define $\mathcal{B}_{ijk}$ as follows, $(0 \le s < (p-1)/2)$.

1. $\mathcal{B}_{i0k}$:

$(i + a, i + b, i + c)_(0, k)$, for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^s, i - \xi^s)_(0, k)$,
$(\infty_1, i + \xi^{4s}, i + \xi^{4s+h})_(0, k)$,
$(\infty_1, i + \xi^{4s+2}, i + \xi^{4s+2+h})_(1, k)$,
$(\infty_2, i + \xi^{4s+1}, i + \xi^{4s+1+h})_(-2, k)$,
$(\infty_2, i + \xi^{4s+3}, i + \xi^{4s+3+h})_(0,k)$.

2. $\mathcal{B}_{i1k}$:

$(i + a, i + b, i + c)_(1, k)$, for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^{4s+1}, i + \xi^{4s+1+h})_(1, k)$,
$(0, i + \xi^{4s+3}, i + \xi^{4s+3+h})_(- 1, k)$,
$(\infty_1, i + \xi^{4s+h}, i + \xi^{4s})_(2, k)$,
$(\infty_1, i + \xi^{4s+2}, i + \xi^{4s+2+h})_(- 2, k)$,
$(\infty_2, i + \xi^{4s}, i - \xi^{4s})_(- 1, k)$,
$(\infty_2, i - \xi^{4s+1}, i + \xi^{4s+1})_(0, k)$.

3. $\mathcal{B}_{i2k}$:

$(i + a, i + b, i + c)_(2, k)$, for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^{4s+1}, i + \xi^{4s+1+h})_(2, k)$,
$(0, i + \xi^{4s+3}, i + \xi^{4s+3+h})_(- 2, k)$,
$(\infty_1, i - \xi^{4s}, i + \xi^{4s})_(0, k)$,
$(\infty_1, i + \xi^{4s+1}, i - \xi^{4s+1})_(1, k)$,
$(\infty_2, i + \xi^{4s}, i + \xi^{4s+h})_(- 1, k)$,
$(\infty_2, i + \xi^{4s+2+h}, i + \xi^{4s+2})_(2, k)$.

4. $\mathcal{B}_{imk}$ $(m = 3,4,\ldots,(u - 1) / 2)$:

$(i + a, i + b, i + c)_(m, k)$ for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^{s}, i - \xi^{s})_(m, k)$,
$(\infty_1, i + \xi^{4s}, i + \xi^{4s+h})_(m, k)$,
$(\infty_1, i + \xi^{4s+2}, i + \xi^{4s+2+h})_(m, k)$,
$(\infty_2, i + \xi^{4s+1}, i + \xi^{4s+1+h})_(- m, k)$,
$(\infty_2, i + \xi^{4s+3}, i + \xi^{4s+3+h})_(- m, k)$.

5. $\mathcal{B}_{imk}$ $(m = (u + 1) / 2, (u + 3) / 2,\ldots,u - 3)$:

$(i + a, i + b, i + c)_(m, k)$ for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^{s}, i - \xi^{s})_(m, k)$,
$(\infty_1, i + \xi^{4s+1}, i + \xi^{4s+1+h})_(- m, k)$,
$(\infty_1, i + \xi^{4s+3}, i + \xi^{4s+3+h})_(- m, k)$,
$(\infty_2, i + \xi^{4s}, i + \xi^{4s+h})_(m, k)$,
$(\infty_2, i + \xi^{4s+2}, i + \xi^{4s+2+h})_(m, k)$.

6. $\mathcal{B}_{i(u-2)k}$:

$(i + a, i + b, i + c)_(u - 2, k)$, for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^{4s}, i + \xi^{4s+h})_(2, k)$,
$(0, i + \xi^{4s+2}, i + \xi^{4s+2+h})_(- 2, k)$,
$(\infty_1, i + \xi^{4s+3}, i + \xi^{4s+3+h})_(2, k)$,
$(\infty_1, i + \xi^{4s+1+h}, i + \xi^{4s+1})_(- 2, k)$,
$(\infty_2, i + \xi^{4s}, i - \xi^{4s})_(1, k)$,
$(\infty_2, \xi^{4s+1}, i - \xi^{4s+1})_(- 2, k)$.

7. $\mathcal{B}_{i(u-1)k}$:

$(i + a, i + b, i + c)_(u - 1, k)$, for $\{a,b,c\} \in \mathcal{S}$, $a < b < c$,
$(0, i + \xi^{4s}, i + \xi^{4s+h})_(1, k)$,
$(0, i + \xi^{4s+2}, i + \xi^{4s+2+h})_(- 1, k)$,
$(\infty_1, i + \xi^{4s+3+h}, i + \xi^{4s+3})_(1, k)$,
$(\infty_1, i + \xi^{4s+1}, i + \xi^{4s+1+h})_(- 1, k)$,
$(\infty_2, i - \xi^{4s}, i + \xi^{4s})_(2, k)$,
$(\infty_2, i - \xi^{4s+1}, i + \xi^{4s+1})_(- 1, k)$.

Let $\mathcal{C}_{ijk} = \mathcal{A}_{ijk} \cup \mathcal{B}_{ijk}$, $i \in Z_p$, $j \in Z_u$, $k \in Z_t$. One can see that each $(V, \mathcal{G}, \mathcal{C}_{ijk})$ is a 3-GD(t^{up+2}), $i \in Z_p$, $j \in Z_u$, $k \in Z_t$. Using Lemma 3.5.1, we can verify that $\mathcal{C}_{ijk}$ ($i \in Z_p$, $j \in Z_u$, $k \in Z_t$) are mutually disjoint. So we have a large set LSDG(t^{up+2}). ◆

Constructing satisfactory STS(p+2) $(X, \mathcal{A})$ useful in Lemma 3.5.2 relies on selecting proper $\mathcal{R}$. We present some constructions in Appendix II. Therefore, we have the following result.

Lemma 3.5.2 Suppose p is prime and $p \equiv 5 \pmod 8$ $p \leq 157$. If $u \geq 5$ and an LSDG(t^{u+2}) exists, then an LSDG(t^{up+2}) exists.

Chapter 4

Tripling Constructions

Main results

1. Suppose there exist an LSDG(t^{2u}) and an LSDG(t^{6}), where $u \neq 2, 6$. Then there exists an LSDG(t^{6u}).
2. Suppose there exist an LSDG($t^{u}s^{1}$) and an LSDG($t^{3}s^{1}$), where $s \geq t$ and $u \neq 2, 6$. Then there exists an LSDG($t^{3u}s^{1}$).

4.1 Introduction

This chapter gives two "tripling" construction in section 4.3 and 4.4 respectively. The content of this chapter has been submitted for publication in [5].

4.2 Preliminaries

Suppose X is a set of size tu and $\mathcal{H}$ is a partition of X into u subsets of size t. A tu by tu square array L, indexed by X, is called a *partitioned incomplete Latin square* (or PILS) of type t^u if L satisfies the following properties

1) if $x, y \in H \in \mathcal{H}$, then L(x, y) is empty; otherwise L(x, y) is an element of X;
2) if $x \in H \in \mathcal{H}$, both row and column x of L contain every element of $X \setminus H$.

Elements of $\mathcal{H}$ are called *holes*. L is said to be *symmetric* if L(x, y) = L(y, x) for all x and y not in the same hole. The following result is proved in [11].

Lemma 4.2.1 ([11]) Suppose t is even and $u \geq 3$. Then a symmetric PILS of type t^u exists.

Suppose $(X, \mathcal{G}, \mathcal{A})$ is a 3-GDD. A subset $\mathcal{P}$ of $\mathcal{A}$ is called a *parallel class* if $\mathcal{P}$ is a partition of X. $(X, \mathcal{G}, \mathcal{A})$ is said to be *resolvable* if $\mathcal{A}$ can be partitioned into parallel classes. It is well known that there exists a resolvable 3-GDD(u^3) if $u \neq 2, 6$.

Suppose $(X, \mathcal{G}, \mathcal{A})$ is a resolvable 3-GDD(u^3) with point set $X = Z_u \times Z_3$ and group set $\mathcal{G} = \{Z_u \times \{g\} : g \in Z_3\}$. For $h \in Z_u$, define $\mathcal{A}_h = \{\{(a, 0), (b, 1), (c + h, 2)\}: \{(a, 0), (b, 1), (c, 2)\} \in \mathcal{A}\}$. Then $(X, \mathcal{G}, \mathcal{A}_h)$ $(h \in Z_u)$ are u disjoint resolvable 3-GDD(u^3)s. Therefore we obtain the following result.

Lemma 4.2.2 For all $u \neq 2, 6$, there exists an LSDG(u^3) with all of its 3-GDD(u^3)s resolvable.

4.3 Construction I

Our first construction is the following.

Lemma 4.3.1 Suppose there exist an LSDG(t^{2u}) and an LSDG(t^6), where $u \neq 2, 6$. Then there exists an LSDG(t^{6u}).

Proof. We employ point set

$$Y = (Z_t \times Z_2 \times Z_u \times Z_3).$$

The group set will be

$$\mathcal{H} = \{Z_t \times \{x\}: x \in Z_2 \times Z_u \times Z_3\}.$$

Let $X = Z_u \times Z_3$. Take u disjoint resolvable 3-GDD(u^3)s $(X, \mathcal{G}, \mathcal{A}_h)$ $(h \in Z_u)$ with $\mathcal{G} = \{Z_u \times \{g\} : g \in Z_3\}$ (by Lemma 4.2.2).

Now we present two methods of constructing 3-GDD(t^{6u})s with group set $\mathcal{H}$. The first method will produce $2t(u - 1)$ disjoint 3-GDD(t^{6u})s. The second will produce $4tu$ disjoint 3-GDD(t^{6u})s. Together they form an LSDG(t^{6u}).

Method one. We use two steps to construct 3-GDD(t^{6u})s by using $\mathcal{A}_h$ ($h \in Z_u \setminus \{0\}$) (the $\mathcal{A}_0$ is saved for Method two).

1) For each h ($h \in Z_u \setminus \{0\}$) do the following. For every $\{x, y, z\} \in \mathcal{A}_h$, take an LSDG($(2t)^3$) on point set $Z_t \times Z_2 \times \{x, y, z\}$, with groups $Z_t \times Z_2 \times \{x\}$, $Z_t \times Z_2 \times \{y\}$, $Z_t \times Z_2 \times \{z\}$. Name the 2t block sets $\mathcal{A}_{ijh}$, $i \in Z_t$, $j \in Z_2$.

2) For each $g \in Z_3$, take an LSDG(t^{2u}) on point set $Z_t \times Z_2 \times Z_u \times \{g\}$, with groups $Z_t \times \{j\} \times \{k\} \times \{g\}$, $j \in Z_2$, $k \in Z_u$. Name the 2t(u - 1) block sets $\mathcal{B}_{ijhg}$, $i \in Z_t$, $j \in Z_2$.

Now define

$$\mathcal{C}_{ijh} = \mathcal{A}_{ijh} \cup \mathcal{B}_{ijh0} \cup \mathcal{B}_{ijh1} \cup \mathcal{B}_{ijh2},$$

$i \in Z_t$, $j \in Z_2$, $h \in Z_u \setminus \{0\}$. We claim $(Y, \mathcal{H}, \mathcal{C}_{ijh})$, $i \in Z_t$, $j \in Z_2$, $h \in Z_u \setminus \{0\}$, are 2t(u - 1) disjoint 3-GDD(t^{6u})s.

Method two. Now we make use of $\mathcal{A}_0$ and its resolvability. Let $\mathcal{P}_h$ ($0 \le h \le u - 1$) be the u parallel classes of $\mathcal{A}_0$. For each $\mathcal{P}_h$, define three permutations of Z_u, namely α_h^g ($g \in Z_3$), by

$$\alpha_h^g(a) = b \text{ if } \{(a, g), (b, g + 1)\} \subseteq B \text{ for some } B \in \mathcal{P}_h.$$

For each $\mathcal{P}_h$, we will construct 4t disjoint 3-GDD(t^{6u})s. We still use two steps here. For each h, $0 \le h \le u - 1$, do the following.

1) Take a symmetric PILS of type $(2t)^u$ having holes $Z_t \times Z_2 \times \{k\}$, $k \in Z_u$ (such a PILS exists by Lemma 4.2.1.)

For $i \in Z_t$, $j \in Z_2$, define a 3-GDD($(6t)^u$) on point set Y, with groups set $Z_t \times Z_2 \times B$, where $B \in \mathcal{P}_h$ (note $\mathcal{P}_h$ is a partition of $Z_u \times Z_3$). Its block set $\mathcal{D}_{ijh1}$ consists of the triples

$$\{(a, b, c, d), (a', b', c', d), (a'' + i, b'' + j, \alpha_h^d(c''), d + 1)\}$$

where $a, a' \in Z_t$, $b, b' \in Z_2$, $c, c' \in Z_u$ and $c < c'$, $d \in Z_3$, and $(a'', b'', c'') = L((a, b, c), (a', b', c'))$.

For $i \in Z_t$, $j \in Z_2$, define another 3-GDD($(6t)^u$) on point set Y, with groups set $Z_t \times Z_2 \times B$, where $B \in \mathcal{P}_h$. The block set $\mathcal{D}_{ijh2}$ consists of the triples

$$\{(a, b, c, d), (a', b', c', d), (a'' + i, b'' + j, (\alpha_h^{d-1})^{-1}(c''), d - 1)\}$$

where $a, a' \in Z_t$, $b, b' \in Z_2$, $c, c' \in Z_u$ and $c < c'$, $d \in Z_3$, and $(a'', b'', c'') = L((a, b, c), (a', b', c'))$.

2) For every $B \in \mathcal{P}_h$, take an LSDG(t^6), on point set $Z_t \times Z_2 \times B$, with groups $Z_t \times \{b\} \times \{(c, d)\}$ where $b \in Z_2$ and $(c, d) \in B$. Name the 4t block sets by $\mathcal{E}(B)_{ijhm}$, $i \in Z_t$, $j \in Z_2$, $m = 1, 2$. Define $\mathcal{E}_{ijhm} = \bigcup_{B \in \mathcal{P}_h} \mathcal{E}(B)_{ijhm}$, $i \in Z_t$, $j \in Z_2$, $m = 1, 2$.

Now let

$$\mathcal{F}_{ijhm} = \mathcal{D}_{ijhm} \cup \mathcal{E}_{ijhm},$$

$i \in Z_t$, $j \in Z_2$, $0 \le h \le u - 1$, $m = 1, 2$. We claim that $(Y, \mathcal{H}, \mathcal{F}_{ijhm})$ are 4tu disjoint 3-GDD(t^{6u})s.

With methods one and two, we get a total of t(6u - 2) 3-GDD(t^u)s. Since they are disjoint, we have an LSDG(t^{6u}). ♦

4.4 Construction II

In this section we modify the construction in section 2 to deal with 3-GDD($t^{3u}s^1$)s with $s \ge t$. Notice the necessary condition for the existence of a 3-GDD(t^3s^1) is that both t and s be even. The result is the following.

Lemma 4.4.1 Suppose there exist an LSDG(t^us^1) and an LSDG(t^3s^1), where $s \ge t$ and $u \ne 2, 6$; then there exists an LSDG($t^{3u}s^1$).

Proof. Let $\Omega = \{\infty_1, ..., \infty_s\}$, We construct 3-GDD($t^{3u}s^1$)s on point set

$$Y = (Z_t \times Z_u \times Z_3) \cup \Omega,$$

with group set $\mathcal{H}$ consisting of

$$Z_t \times \{k\} \times \{g\} \ (k \in Z_u, g \in Z_3), \text{ and } \Omega.$$

Let $X = Z_u \times Z_3$. As before, take u disjoint resolvable 3-GDD(u^3)s $(X, \mathcal{G}, \mathcal{A}_h)$ $(h \in Z_u)$ with $\mathcal{G} = \{Z_u \times \{g\} : g \in Z_3\}$ (by Lemma 4.2.2).

Now we display two methods to construct disjoint 3-GDD($t^{3u}s^1$)s with point set Y and group set $\mathcal{H}$. The first method will produce t(u - 1) such GDDs. The second will produce another 2tu. Together they form an LSDG($t^{3u}s^1$).

Method one. We use two steps to construct 3-GDD($t^{3u}s^1$)s by using $\mathcal{A}_h$ $(h \in Z_u \setminus \{0\})$ (the $\mathcal{A}_0$ is saved for Method two).

1) For each h $(h \in Z_u \setminus \{0\})$ do the following. For every $\{x, y, z\} \in \mathcal{A}_h$, take an LSDG($t^3$) on point set $Z_t \times \{x, y, z\}$, with groups $Z_t \times \{x\}$, $Z_t \times \{y\}$, $Z_t \times \{z\}$. Name the t block sets $\mathcal{A}_{ih}$, $i \in Z_t$.
2) For each $g \in Z_3$, take an LSDG($t^u s^1$) on point set $(Z_t \times Z_u \times \{g\}) \cup \Omega$, with groups $Z_t \times \{k\} \times \{g\}$ $(k \in Z_u)$, and Ω. Name the t(u - 1) block sets $\mathcal{B}_{ihg}$, $i \in Z_t$, $h \in Z_u \setminus \{0\}$.

Now define

$$\mathcal{C}_{ih} = \mathcal{A}_{ih} \cup \mathcal{B}_{ih0} \cup \mathcal{B}_{ih1} \cup \mathcal{B}_{ih2},$$

$i \in Z_t$, $h \in Z_u \setminus \{0\}$. We claim $(Y, \mathcal{H}, \mathcal{C}_{ih})$, where $i \in Z_t$ and $h \in Z_u \setminus \{0\}$, are t(u - 1) disjoint 3-GDD($t^{3u}s^1$)s.

Method two. As in the proof of Lemma 4.3.1, we make use of $\mathcal{A}_0$ and its resolvability here. Let $\mathcal{P}_h$ $(0 \le h \le u - 1)$ be the u parallel classes of $\mathcal{A}_0$. For any $\mathcal{P}_h$ define three permutations of Z_u, namely α_h^g $(g \in Z_3)$, as follows:

$$\alpha_h^g(a) = b \text{ if } \{(a, g), (b, g + 1)\} \subseteq B \text{ for some } B \in \mathcal{P}_h.$$

For each $\mathcal{P}_h$, we shall construct 2t disjoint 3-GDD($t^{3u}s^1$)s. We still use two steps here. For each h $(0 \le h \le u - 1)$ do the following.

1) Take a symmetric PILS of type t^u having holes $Z_t \times \{k\}$, $k \in Z_u$ (such a PILS exists by Lemma 4.2.1, for t is even.)

For $i \in Z_t$, define a 3-GDD$((3t)^u)$ on point set $Y \setminus \Omega$, with groups set $Z_t \times B$, where $B \in \mathcal{P}_h$ (note $\mathcal{P}_h$ is a partition of $Z_u \times Z_3$). Its block set $\mathcal{D}_{ih1}$ consists of the triples

$$\{(a, c, d), (a', c', d), (a'' + i, \alpha_h^d(c''), d + 1)\}$$

where $a, a' \in Z_t$, $c, c' \in Z_u$ and $c < c'$, $d \in Z_3$, and $(a'', c'') = L((a, c), (a', c'))$.
For $i \in Z_t$, define another 3-GDD$((3t)^u)$ on point set $Y \setminus \Omega$, with groups set $Z_t \times B$, where $B \in \mathcal{P}_h$. The block set $\mathcal{D}_{ih2}$ consists of the triples

$$\{(a, c, d), (a', c', d), (a'' + i, (\alpha_h^{d-1})^{-1}(c''), d - 1)\}$$

where $a, a' \in Z_t$, $c, c' \in Z_u$ and $c < c'$, $d \in Z_3$, and $(a'', c'') = L((a, c), (a', c'))$.

2) For every $B \in \mathcal{P}_h$, take an LSDG(t^3s^1), on point set $(Z_t \times B) \cup \Omega$, with groups $Z_t \times \{(c, d)\}$, where $(c, d) \in B$, and Ω. Name the $2t$ block sets $\mathcal{E}(B)_{ihm}$, $i \in Z_t$, $m = 1, 2$. Define $\mathcal{E}_{ihm} = \bigcup_{B \in \mathcal{P}_h} \mathcal{E}(B)_{ihm}$, $i \in Z_t$, $m = 1, 2$.

Now let

$$\mathcal{F}_{ihm} = \mathcal{D}_{ihm} \cup \mathcal{E}_{ihm},$$

$i \in Z_t$, $0 \le h \le u - 1$, $m = 1, 2$. We claim that $(Y, \mathcal{H}, \mathcal{F}_{ihm})$ are $2tu$ disjoint 3-GDD$(t^3u_s^1)$s.

Triples constructed in Method one and two are distinct. They form $t(3u - 1)$ disjoint 3-GDD$(t^3u_s^1)$s, a large set. ♦

Chapter 5

The Doubling Construction

Main Result

Suppose $u \geq 4$ is even and $t \in \{3, 6\}$. If an LSDG(t^{u-1}) exists, then there exists an LSDG(t^{2u-1}).

5.1 Introduction

This chapter establishes Rosa's Theorem, a "doubling" construction for large sets of disjoint 3-GDDs. Section 5.2 introduces a kind of array and does some preliminaries. Section 5.3 establishes a recursive construction. Section 5.4 is a preparation for section 5.5. Section 5.5 deals with the existence of arrays. The result is presented in section 5.6.

5.2 Preliminaries

Suppose M is a set of size t(u - 1). A tu by tu square array S, indexed by 1, ..., tu, is called an *ARRAY* of type t^u if S satisfies the following two conditions:

1) if $|i - j| \geq t$ then S(i, j) is an element of M; otherwise S(i, j) is empty;
2) each element of M appears in every row and every column of S exactly once.

An ARRAY of type t^u is denoted by $A(t^u)$. It has u square t by t "holes" along its main diagonal. An $A(t^u)$ S is said to be *symmetric* if S(i, j) = S(j, i) for $|i - j| \geq t$. An $A(t^u)$ S is said to be *anti-symmetric* if $S(i, j) \neq S(j, i)$ whenever $|i - j| \geq t$. Two $A(t^u)$, S and T, are said to be *disjoint* if $S(i, j) \neq T(i, j)$ and $S(i, j) \neq T(j, i)$ whenever $|i - j| \geq t$.

A set of t(u - 2) disjoint $A(t^u)$ with t(u -3) of them symmetric and the remaining t of them anti-symmetric is called *a large set* of disjoint $A(t^u)$, and is denoted by $LA(t^u)$. $LA(t^u)$ is useful in the constructions of this chapter, whose existence is discussed in section 5.5.

Example. The following is an LA(1^6). The first is anti-symmetric, the next three are symmetric, where M = {A, B, C, D, E}.

	A	B	C	D	E
B		A	E	C	D
A	B		D	E	C
D	C	E		A	B
E	D	C	B		A
C	E	D	A	B	

	E	D	A	C	B
E		C	D	B	A
D	C		B	A	E
A	D	B		E	C
C	B	A	E		D
B	A	E	C	D	

	C	E	B	A	D
C		D	A	E	B
E	D		C	B	A
B	A	C		D	E
A	E	B	D		C
D	B	A	E	C	

	D	C	E	B	A
D		E	B	A	C
C	E		A	D	B
E	B	A		C	D
B	A	D	C		E
A	C	B	D	E	

Suppose X is a set of size tu. An H(u, t, k, s)-*system* (briefly H(u, t, k, s)) is (X, $\mathcal{G}$, $\mathcal{B}$) such that

1) $\mathcal{G}$ is a partition of X into u subsets of size t called *groups*
2) $\mathcal{B}$ is a set of k-subsets of X called *blocks*, such that a block contains at most one common point with a group, and every s points from s different groups occur in a unique block.

H(u,t,k,s) is a generalization of group-divisible designs. The main results about H(u, t, 4, 3) are from [12], [22] and [13].

Lemma 5.2.1 (1) [12] An H(u, 1, 4, 3) exists if and only if $u \geq 4$ and $u \equiv 2, 4 \pmod 6$.
(2) [22] An H(u, 3, 4, 3) exists if and only if $u \geq 4$ and $u \equiv 0 \pmod 6$.
(3) [13] An H(u, 6, 4, 3) exists if and only if $u \geq 4$ with possible exceptions u = 9, 27 and 81.

Proof. (1) is from [12]. (3) is from [13]. [22] implicitly gives (2). The simple process is as follows. [22] has shown that, if X is a set of u points, $u \equiv 0 \pmod 6$, then there exists a collection $\mathcal{B}$ of subset of X such that

1) every element of $\mathcal{B}$ has size 4 or 6;
2) every triple of X is contained in exactly one element of $\mathcal{B}$.

Making 3 copies of every point in X and using the ingredient designs H(4, 3, 4, 3), which exists since an H(4, 1, 4, 3) exists, and H(6, 3, 4, 3), which is given in [22], we have an H(u, 3, 4, 3). ◆

5.3 The main construction

In our constructions, we use two disjoint sets, M and N. M is of size t(u - 1) and N of size tu. Both M and N are partitioned into subsets of size t, say

$$M = \bigcup_{1 \le k \le u-1} M_k$$

and

$$N = \bigcup_{1 \le k \le u} N_k.$$

For convenience, we take

$$N = \{i : \text{integer } i,\ 1 \le i \le tu\}$$

and

$$N_k = \{i : \text{integer } i,\ (k - 1)t + 1 \le i \le kt\}$$

where $1 \le k \le u$.

Entries of $A(t^u)$ are empty or elements of M. Every $A(t^u)$ is indexed with elements of N. First we use symmetric $A(t^u)$ in the construction.

Lemma 5.3.1 Suppose there is an LSDG(t^{u-1}). If there are t(u - 3) disjoint symmetric $A(t^u)$, then there are t(u -3) disjoint 3-GDD(t^{2u-1}).

Proof. We construct 3-GDD(t^{2u-1}) on

$$X = M \cup N$$

with group set

$$\mathcal{G} = \{M_k : 1 \le k \le u - 1\} \cup \{N_k : 1 \le k \le u\}.$$

Take an LSDG(t^{u-1}) on point set M with groups M_k ($1 \le k \le u - 1$). Suppose the t(u - 3) block sets are $\mathcal{A}_r$, $1 \le r \le t(u - 3)$. Suppose S_r ($1 \le r \le t(u - 3)$) are t(u - 3) disjoint symmetric $A(t^u)$ on M. For each r, $1 \le r \le t(u - 3)$, let $\mathcal{B}_r$ consist of blocks of the following two types

type 1) all the blocks in $\mathcal{A}_r$

type 2) $\{i, j, S_r(i, j)\}$ if $i < j$ and $|i - j| \geq t$.

It is easy to see that $(X, \mathcal{G}, \mathcal{B}_r)$ $(1 \leq r \leq t(u - 3))$ are disjoint 3-GDD(t^{2u-1}). ◆

Now we use t disjoint anti-symmetric A(t^u). The construction is quite complicated. We need some preliminaries.

Suppose S_k, $1 \leq k \leq t$, are t disjoint anti-symmetric A(t^u) on M. Every S_k can be viewed as a u by tu (u rows and tu coloumns) array whose entries are column vectors of length t. In this view, S_k is denoted by $\overline{S}_k$. S_k and $\overline{S}_k$ are the same but under different views.

As an ingredient design, we need a resolvable 2-GDD(t^u).

If tu is even, then a resolvable 2-GDD(t^u) exists (see [7]). Let $\Omega = \{\infty_1, ..., \infty_t\}$. Take a resolvable 2-GDD(t^u) with groups M_k $(1 \leq k \leq u - 1)$ and Ω. This resolvable 2-GDD(t^u) has t(u - 1) parallel classes, say $\mathcal{P}_k$ $(1 \leq k \leq t(u - 1))$. Divide each $\mathcal{P}_k$, $1 \leq k \leq t(u - 1)$, into two parts

$$\mathcal{P}_k^{(1)} = \{\{x, m\}: x \in \Omega, m \in M, \{x, m\} \in \mathcal{P}_k\}$$
$$\mathcal{P}_k^{(2)} = \mathcal{P}_k \setminus \mathcal{P}_k^{(1)}.$$

From $\mathcal{P}_k^{(1)}$ we define a column vector $\overline{v}_k = (m_1, m_2, ..., m_t)^T$, where $\{\infty_i, m_i\} \in \mathcal{P}_k^{(1)}$.

Let

$$V = \{\overline{v}_k : 1 \leq k \leq t(u - 1)\}.$$

Define a mapping φ from set V to a set of pairs of M by $\varphi(\overline{v}_k) = \mathcal{P}_k^{(2)}$, $1 \leq k \leq t(u - 1)$.

Anti-symmetric A(t^u) S_k $(1 \leq k \leq t)$ are said to be *associated with* the above resolvable 2-GDD(t^u) if they posess the following properties:

(5.3.1) every entry of each $\overline{S}_k$ is empty or an element of V;

(5.3.2) every element of V appears exactly once in every row of each $\mathbb{S}_k$;

(5.3.3) every element of V appears in column j of exactly one of the $\mathbb{S}_k$ $(1 \le k \le t)$, for every $1 \le j \le tu$.

Example. The following is an $LA(2^4)$, whose two symmetric $A(2^4)$ and two anti-symmetric $A(2^4)$ are derived from the first and second $A(2^4)$ below, respectively, using the permutation (A, B)(C, E)(D, F), where M = {A, B, C, D, E, F}.

	AB	CD	EF
	BA	DC	FE
EF		AB	CD
FE		BA	DC
DC	EF		AB
CD	FE		BA
AB	DC	EF	
BA	CD	FE	

	DC	AB	FE
	CD	BA	EF
DC		FE	AB
CD		EF	BA
AB	FE		DC
BA	EF		CD
FE	AB	DC	
EF	BA	CD	

The two anti-symmetric $A(2^4)$, say S_1 and S_2, are associated with a resolvable 2-GDD(2^4) with groups $\{\infty_1, \infty_2\}$, {A, B}, {C, D}, {E, F}. We list the 6 parallel classes of the resolvable 2-GDD(2^4) in Table 5.3.1. Every entry of $\mathbb{S}_k$, $1 \le k \le 2$, is mapped by φ to a set of pairs of M. For instance, all the entries with $(C, D)^T$ are mapped to {{A, E},{B, F}}.

		k = 1	k = 2	k = 3	k = 4	k = 5	k = 6
$\mathbb{P}_k$	$\mathbb{P}_k^{(1)}$	$\{\infty_1, A\}$ $\{\infty_2, B\}$	$\{\infty_1, B\}$ $\{\infty_2, A\}$	$\{\infty_1, C\}$ $\{\infty_2, D\}$	$\{\infty_1, D\}$ $\{\infty_2, C\}$	$\{\infty_1, E\}$ $\{\infty_2, F\}$	$\{\infty_1, F\}$ $\{\infty_2, E\}$
	$\mathbb{P}_k^{(2)}$	{C, E} {D, F}	{C, F} {D, E}	{A, E} {B, F}	{A, F} {B, E}	{A, C} {B, D}	{A, D} {B, C}

Table 5.3.1

Now we show how to construct tu disjoint 3-GDD(t^{2u-1}) using t anti-symmetric $A(t^u)$ associated with a resolvable 2-GDD(t^u).

Lemma 5.3.2 Suppose there is an H(u, t, 4, 3). If there are t anti-symmetric $A(t^u)$ associated with a resolvable 2-GDD(t^u), then there are tu disjoint 3-GDD(t^{2u-1}).

Proof. We construct 3-GDD(t^{2u-1}) on

$$X = M \cup N$$

with group set

$$\mathcal{G} = \{M_k : 1 \le k \le u - 1\} \cup \{N_k : 1 \le k \le u\}.$$

Take an H(u, t, 4, 3) on N with groups N_k ($1 \le k \le u$). Suppose $\mathcal{H}$ is the block set (each block has size 4). Suppose S_k, $1 \le k \le t$, are t anti-symmetric $A(t^u)$ associated with a resolvable 2-GDD(t^u) with u groups M_k ($1 \le k \le u - 1$) and Ω, where $\Omega = \{\infty_1, ..., \infty_t\}$. We construct one 3-GDD(t^{2u-1}) from each of the u rows of every S_k ($1 \le k \le t$).

For $1 \le u' \le u$ and $1 \le t' \le t$, do the following. Let $r = (u' - 1)t + t'$. Then $r \in N_{u'}$. Let $\mathcal{H}_r = \{\{a, b, c\}: \{r, a, b, c\} \in \mathcal{H}\}$. Then

$$(N \setminus N_{u'}, \{N_k : 1 \le k \le u, k \ne u'\}, \mathcal{H}_r)$$

is a 3-GDD(t^{u-1}). Let $\mathcal{B}_r$ consist of blocks of the following three types:

type 1) $\{j, x, y\}$, for $1 \le j \le tu$, $j \notin N_{u'}$ and $\{x, y\} \in \varphi(S_{t'}(u', j))$;
type 2) $\{i, j, S_{t'}(i, j)\}$, for $i \in N_{u'}$, $1 \le j \le tu$ and $j \notin N_{u'}$;
type 3) $\{a, b, c\}$ in $\mathcal{H}_r$.

There are $\frac{1}{2}t^2(u - 1)(u - 2)$ blocks of type 1, $t^2(u - 1)$ of type 2, $\frac{1}{6}t^2(u - 1)(u - 2)$ of type 3. Now we show that $(X, \mathcal{G}, \mathcal{B}_r)$, $1 \le r \le tu$, are disjoint 3-GDD(t^{2u-1}).

First we show that $(X, \mathcal{G}, \mathcal{B}_r)$ is a 3-GDD(t^{2u-1}). For $i \in N_{u'}$, $j \notin N_{u'}$, $\{i, j\}$ occurs in a block of type 2. For $i, j \notin N_{u'}$ and not in the same group (i.e. $|i - j| \ge t$), $\{i, j\}$ occurs in a block of type 3. For $x, y \in M$ and not in the same group, $\{x, y\}$ occurs in a block of type 1 (from association property 2). For $x \in M$, $i \in N_{u'}$, $\{x, i\}$ is in a block of type 2. For $x \in M$ and $j \notin N_{u'}$, $\{x, j\}$ is in a block of type 1 or 2.

Then we show that the constructed $\mathcal{B}_r$ ($1 \le r \le tu$) are disjoint. We note that any block of type 1 has one point in N; of type 2 has two points in N; of type 3 has three points in N. Type 3 cannot produce repeated blocks. Since S_k ($1 \le k \le t$) are disjoint and anti-

symmetric, type 2 cannot produce repeated blocks. Type 1 cannot produce repeated blocks (from association property 3). Therefore, $\mathcal{B}_r$ $(1 \le r \le tu)$ are disjoint. ♦

Lemma 5.3.3 If t(u - 3) symmetric $A(t^u)$ used in Lemma 5.3.1 and t anti-symmetric $A(t^u)$ used in Lemma 5.3.2 are disjoint, then all 3-GDD(t^{2u-1}) constructed in Lemma 5.3.1 and Lemma 5.3.2 are disjoint.

Proof. Blocks of type 1 in Lemma 5.3.1 have no point in N. So, they will not appear in any 3-GDD(t^{2u-1}) constructed in Lemma 5.3.2. Blocks of type 2 in Lemma 5.3.1 will not appear in Lemma 5.3.2, since the $A(t^u)$ used are disjoint. ♦

Therefore, we obtain the following.

Lemma 5.3.4 Suppose an H(u, t, 4, 3) exists. Suppose there exists an $LA(t^u)$ with its N-symmetric $A(t^u)$ associated with a resolvable 2-GDD(t^u). Then an LSDG(t^{2u-1}) exists provided with an LSDG(t^{u-1}).

In the rest of this chapter (mainly section 5.5), we will deal with the existence of an $LA(t^u)$ associated with a resolvable 2-GDD(t^u). Section 5.4 is a preparation for section 5.5.

5.4 A lemma about one-factorization

This section prepares a fact which is used in section 5.5.

A resolvable 2-GDD(t^u) exists if and only if $tu \equiv 0 \pmod 2$. View a block {x, y} as an edge xy; then a resolvable 2-GDD(t^u) is a one-factorization of a u-partite graph with every parallel class as a one-factor. Denote by $f(t^u)$ the maximum number of parallel classes (of a resolvable 2-GDD(t^u)) whose union is a bipartite graph. In [23], it is shown that $f(1^2) = 1$, $f(1^4) = f(1^6) = 2$ and $f(1^u) \ge 3$ for even $u \ge 8$. In this section we evaluate $f(t^u)$ in Lemma 5.4.1, which will be used in next section.

A *Skolem k-sequence* is a set of k disjoint pairs $\{p_r, q_r\}$ covering the elements of {1, 2, ..., 2k} exactly once and such that $q_r - p_r = r$ for r = 1, 2, ..., k. It is well known that a Skolem k-sequence exists if and only if $k \equiv 0$ or 1 (mod 4). A *weak* Skolem k-sequence is a set of k - 1 disjoint pairs $\{p_r, q_r\}$ such that $q_r - p_r = r$ for r = 1, 2, ..., k - 1, and it covers the elements

of $\{1, 2, ..., 2k\} \setminus \{d_1, d_2\}$ for some $d_1, d_2 \in \{1, 2, ..., 2k\}$. For $k \equiv 2$ or 3 (mod 4), a weak Skolem k-sequence is exhibited in the following.

For $k \equiv 2 \pmod 4$. Let $2k = 8v + 4$. Sequence: $\{1, 2\}$, $\{4v + 2 - i, 4v + 4 + i\}$ for $0 \le i \le 2v - 1$, $\{6v + 5 + j, 2v + 2 - j\}$ for $0 \le j \le 2v - 1$ form a weak Skolem k-sequence, which covers all elements but $d_1 = 4v + 3$ and $d_2 = 6v + 4$.

For $k \equiv 3 \pmod 4$. Let $2k = 8v + 6$. Sequence: $\{1, 2\}$, $\{4v + 3 - i, 4v + 5 + i\}$ for $0 \le i \le 2v$, $\{6v + 7 + j, 2v + 2 - j\}$ for $0 \le j \le 2v - 1$ form a weak Skolem k-sequence, which covers all elements but $d_1 = 4v + 4$ and $d_2 = 6v + 6$.

A Skolem k-sequence is a weak Skolem k-sequence if we let $d_1 = p_k$ and $d_2 = q_k$. So for every positive integer k, there is a weak Skolem k-sequence.

Lemma 5.4.1 (1) if $t \equiv 0 \pmod 2$ and $u \equiv 0 \pmod 2$, then $f(t^u) = tu / 2$
(2) if $t \equiv 0 \pmod 2$ and $u \equiv 1 \pmod 2$, then $f(t^u) = t(u - 1) / 2$
(3) if $t \equiv 1 \pmod 2$ and $u \equiv 0 \pmod 4$, then $f(t^u) = tu / 2$
(4) if $t \equiv 1 \pmod 2$ and $u \equiv 2 \pmod 4$, then $f(t^u) = tu / 2 - 1$.

Proof. First we prove (1) and (3). A complete bipartite graph of tu vertices has $(ut / 2)^2$ edges, which can be the union of at most $tu / 2$ parallel classes. Therefore $f(t^u) \le tu / 2$.

To prove $f(t^u) \ge tu / 2$, we construct a resolvable 2-GDD(t^u) with $tu / 2$ parallel classes forming a complete bipartite graph. We take point set $X = Z_{ut/2} \times Z_2$ and form the groups $\{(a, \varepsilon) : a \in Z_{ut/2}$ and $a \equiv i \pmod{u / 2}\}$ for $\varepsilon \in Z_2$ and $i = 0, 2, ..., u / 2 - 1$.

The blocks are of three types:

type I. $\{(x, 0), (y, 1)\}$ for all $x, y \in Z_{ut/2}$;

type II. all blocks of a resolvable 2-GDD($t^{u/2}$) on $Z_{ut/2} \times \{0\}$ with groups : $\{(a, 0) : a \in Z_{ut/2}$ and $a \equiv i \pmod{u / 2}\}$ for $i = 0, 2, ..., u / 2 - 1$;

type III. all blocks of a resolvable 2-GDD($t^{u/2}$) on $Z_{ut/2} \times \{1\}$ with groups : $\{(a, 1) : a \in Z_{ut/2}$ and $a \equiv i \pmod{u / 2}\}$ for $i = 0, 2, ..., u / 2 - 1$.

Blocks of type I form tu / 2 parallel classes: $\{\{(x, 0), (x + i, 1)\} : x \in Z_{ut/2}\}$, $i \in Z_{ut/2}$, whose union is a bipartite graph. Blocks of type II and Type III can be partitioned into t(u - 2) / 2 parallel classes in the following way. Each parallel class of type II (on set $Z_{ut/2} \times \{0\}$) together with a parallel class of type III (on set $Z_{ut/2} \times \{1\}$) will form a parallel class.

(2). Suppose H is a bipartite graph formed by $f(t^u)$ parallel classes of a resolvable 2-GDD(t^u). Suppose V_1 and V_2 are vertex sets of the two parts of H. Since u is odd, there is one group $G = \{x_1, ..., x_t\}$ which is not contained wholly in V_1 or V_2. Suppose $\{x_1, ..., x_h\} \subseteq V_1$ and $\{x_{h+1}, ..., x_t\} \subseteq V_2$, $0 < h < t$. Without loss of generality, we assume $h \geq t / 2$. Hence $\{x_t, x_1\}, ..., \{x_t, x_h\}$ are not edges of H. Therefore $f(t^u) \leq tu / 2 - h \leq t(u - 1) / 2$.

To prove $f(t^u) \geq t(u - 1) / 2$, we construct a resolvable 2-GDD(t^u) with t(u - 1) / 2 parallel classes forming a bipartite graph. First we deal with the case t = 2.

Let point set be $X = (Z_{u-1} \cup \{\infty\}) \times Z_2$. Let the groups be $\{(\infty, 0), (\infty, 1)\}$, $\{(x, \varepsilon), (x + (u - 1) / 2, \varepsilon)\}$ for $0 \leq x \leq (u - 1) / 2 - 1$ and $\varepsilon \in Z_2$. Let $k = (u - 1) / 2$. Take a weak Skolem k-sequence.

The blocks are of two types:

type I. $\{(x, 0), (y, 1)\}$ for $x, y \in Z_{u-1} \cup \{\infty\}$ and $x \neq y$;

type II. $\{(\infty, \varepsilon), (d_1, \varepsilon)\}$ for $\varepsilon = 0, 1$ (mod u - 1, -)
$\{(d_2, 0), (d_2, 1)\}$ (mod u - 1, -)
$\{(p_r, \varepsilon), (q_r, \varepsilon)\}$ for $1 \leq r \leq k - 1$ (mod u - 1, -).

Blocks of type I can be partitioned into u - 1 parallel classes, whose union is a bipartite graph. Blocks of type II can be partitioned into u - 1 parallel classes.

Therefore $f(2^u) \geq u - 1$. To prove $f(t^u) \geq t(u - 1) / 2$ for t even, we make t / 2 copies for each point in the above constructed resolvable 2-GDD(2^u) and in this way we expand (inflate) the block family to obtain a resolvable 2-GDD(t^u) with t(u - 1) / 2 parallel classes forming a bipartite graph.

(4). If $f(t^u) = tu / 2$, then the tu / 2 parallel classes of a resolvable 2-GDD(t^u) will form a complete bipartite graph H. Suppose V_1 and V_2 are vertex sets of the two parts of H. So,

each parallel class not imbedded in H produces a partition of V_1 and a partition of V_2. But this contradicts the fact that $|V_1| = |V_2| = tu / 2$ (odd). Therefore $f(t^u) \leq tu / 2 - 1$.

To prove $f(t^u) \geq tu / 2 - 1$, we construct a resolvable 2-GDD(t^u) with $tu / 2 - 1$ parallel classes forming a bipartite graph. We construct on $X = (Z_{(u-2)t/2} \cup \{\infty_1, ..., \infty_t\}) \times Z_2$. The groups are $\{(\infty_i, \varepsilon), ..., (\infty_t, \varepsilon)\}$ for $\varepsilon \in Z_2$, and $\{(x, \varepsilon) : x \equiv i \pmod{(u - 2) / 2}\}$ for $0 \leq i \leq (u - 2) / 2 - 1$ and $\varepsilon \in Z_2$. Let $k = t(u - 2) / 4$ and take a weak Skolem k-sequence. Then the blocks are of two types:

type I. $\{(x, 0), (y,1)\}$ for $x, y \in Z_{(u-2)t/2} \cup \{\infty_1, .., \infty_t\}$ and $x \neq y$;

type II. $\{(p_r, \varepsilon), (q_r, \varepsilon)\}$ for $\varepsilon \in Z_2$, $r \neq i((u - 2) / 2)$,
$1 \leq i \leq (t - 1) / 2$, (mod $t(u - 2) / 2$, -);

$\{(\infty_i, \varepsilon), (p_r, \varepsilon)\}$ for $\varepsilon \in Z_2$, $r = i(u - 2) / 2$,
$1 \leq i \leq (t - 1) / 2$, (mod $t(u - 2) / 2$, -);

$\{(\infty_{i+(t-1)/2}, \varepsilon), (q_r, \varepsilon)\}$ for $\varepsilon \in Z_2$, $r = i(u - 2) / 2$,
$1 \leq i \leq (t - 1) / 2$, (mod $t(u - 2) / 2$, -);

$\{(\infty_t, \varepsilon), (d_1, \varepsilon)\}$ for $\varepsilon \in Z_2$ (mod $t(u - 2) / 2$, -);
$\{(d_2, 0), (d_2, 1)\}$ (mod $t(u - 2) / 2$, -);

type III. $\{(\infty_i, 0), (\infty_i, 1)\}$ for $1 \leq i \leq t$;
$\{(0, \varepsilon), (k, \varepsilon)\}$ for $\varepsilon \in Z_2$ (mod $t(u - 2) / 2$, -).

Blocks of type I can be partitioned into $tu / 2 - 1$ parallel classes whose union is a bipartite graph. Blocks of type III is a parallel class. Blocks of type II can be partitioned into $t(u - 2) / 2$ parallel classes. This completes our proof. ♦

5.5 Results on LA(t^u)

Lemma 5.5.1 Suppose $u \geq 4$. Then an LA(t^u) exists only if $tu \equiv 0 \pmod 2$.

Proof. Since $u \geq 4$, there are $t(u - 3)$ symmetric $A(t^u)$ in an $LA(t^u)$. Suppose S is one of them (on M). For $x \in M$, $\{\{i, j\}: i < j \text{ and } S(i, j) = x\}$ is a partition of $N = \{i : i \text{ integer}, 1 \leq i \leq tu\}$. Hence tu is even. ◆

A *Latin square* on a set X, $| X | = w$, is a w by w square such that every element of X appears in each row and each column. The (i, j)th entry of a Latin square L is denoted by L_{ij}. L is said to be *symmetric* if $L_{ij} = L_{ji}$, $1 \leq i \leq j \leq w$.

Lemma 5.5.2 If there is an $LA(t^u)$, then there is an $LA((tw)^u)$ for integer $w \geq 1$. If the $LA(t^u)$ is associated with a resolvable 2-$GDD(t^u)$, then the $LA((tw)^u)$ is associated with a resolvable 2-$GDD((tw)^u)$.

Proof. Suppose S_k, $1 \leq k \leq t(u - 2)$, form the $LA(t^u)$.We construct an $LA((tw)^u)$ on $M \times Z_w$. Let L be a symmetric Latin square on Z_w defined by $L_{ij} = i + j \pmod w$. Rotating columns of L by the permutation (0, 1, ..., w-1), we have w disjoint symmetric Latin squares, denoted by L_h, $1 \leq h \leq w$. Then $S_k \times L_h$, (i.e., replace $(S_k)(i, j)$ by $(S_k)(i, j) \times L_h$), $1 \leq k \leq t(u - 2)$, $1 \leq h \leq w$, form an $LA((tw)^u)$.

Let $(\Omega \cup M, \mathcal{G}, \mathcal{B})$ be a resolvable 2-$GDD(t^u)$ associated with the $LA(t^u)$, where $\Omega = \{\infty_1, ..., \infty_w\}$. Its groups are Ω and M_k, $1 \leq k \leq u - 1$, and $\mathcal{B}$ is partitioned into parallel classes $\mathcal{P}_q$, $1 \leq q \leq t(u - 1)$.

Now we construct a resolvable 2-$GDD((tw)^u)$ on set $(\Omega \cup M) \times Z_w$, with groups $G \times Z_w$ for $G \in \mathcal{G}$. The blocks are $\{(x, i), (y, j)\}$ whenever $\{x, y\} \in \mathcal{B}$ and $i \in Z_w$ and $j \in Z_w$. The $t(u - 1)w$ parallel classes are $\mathcal{P}_{qj}$, $\mathcal{P}_{qj} = \{\{(x, i), (y, L_{ij})\} : \{x, y\} \in \mathcal{P}_q, 1 \leq i \leq w\}$, $1 \leq q \leq t(u - 1)$ and $1 \leq j \leq w$. Thus constructed resolvable 2-$GDD((tw)^u)$ is associated with the constructed $LA((tw)^u)$. ◆

Lemma 5.5.3 $LA(1^4)$ does not exist. There exists an $LA(t^4)$ associated with a resolvable 2-$GDD(t^4)$, $t = 2, 3$.

Proof. It is not difficult to verify that an $LA(1^4)$ does not exist. An $LA(2^4)$ associated with a resolvable 2-$GDD(2^4)$ is given by the Example in Section 5.3. Now we construct an $LA(3^4)$ associated with a resolvable 2-$GDD(3^4)$. Let $M = \{A, B, C, D, E, F, G, H, I\}$. The following is an $LA(3^4)$, whose three symmetric $A(3^4)$ and three anti-symmetric $A(3^4)$ are

derived from the first and second $A(3^4)$ below, respectively, by using permutation (A, D, G)(B, E, H)(C, F, I).

	BCA	DEF	IGH
	CAB	EFD	GHI
	ABC	FDE	HIG
GHI		BCA	DEF
HIG		CAB	EFD
IGH		ABC	FDE
FDE	GHI		BCA
DEF	HIG		CAB
EFD	IGH		ABC
BCA	FDE	IGH	
CAB	DEF	GHI	
ABC	EFD	HIG	

	CAB	EFD	GHI
	ABC	FDE	HIG
	BCA	DEF	IGH
CAB		IGH	EFD
ABC		GHI	FDE
BCA		HIG	DEF
EFD	IGH		ABC
FDE	GHI		BCA
DEF	HIG		CAB
GHI	EFD	ABC	
HIG	FDE	BCA	
IGH	DEF	CAB	

The three anti-symmetric $A(3^4)$ are associated with a resolvable 2-GDD(3^4) with groups $\{\infty_1, \infty_2, \infty_3\}$, {A, B, C}, {D, E, F}, {G, H, I}. We list the 9 parallel classes of the resolvable 2-GDD(3^4) in Table 5.5.1. ♦

		k = 1	k = 2	k = 3	k = 4	k = 5	k = 6	k = 7	k = 8	k = 9
$\mathbb{P}_k$	$\mathbb{P}_k^{(1)}$	$\{\infty_1, A\}$	$\{\infty_1, C\}$	$\{\infty_1, B\}$	$\{\infty_1, D\}$	$\{\infty_1, F\}$	$\{\infty_1, E\}$	$\{\infty_1, G\}$	$\{\infty_1, I\}$	$\{\infty_1, H\}$
		$\{\infty_2, B\}$	$\{\infty_2, A\}$	$\{\infty_2, C\}$	$\{\infty_2, E\}$	$\{\infty_2, D\}$	$\{\infty_2, F\}$	$\{\infty_2, H\}$	$\{\infty_2, G\}$	$\{\infty_2, I\}$
		$\{\infty_3, C\}$	$\{\infty_3, B\}$	$\{\infty_3, A\}$	$\{\infty_3, F\}$	$\{\infty_3, E\}$	$\{\infty_3, D\}$	$\{\infty_3, I\}$	$\{\infty_3, H\}$	$\{\infty_3, G\}$
	$\mathbb{P}_k^{(2)}$	{D, G}	{D, I}	{D, H}	{G, A}	{G, C}	{G, B}	{A, D}	{A, F}	{A, E}
		{E, H}	{E, G}	{E, I}	{H, B}	{H, A}	{H, C}	{B, E}	{B, D}	{B, F}
		{F, I}	{F, H}	{F, G}	{I, C}	{I, B}	{I, A}	{C, F}	{C, E}	{C, D}

Table 5.5.1

Lemma 5.5.4 If $tu \equiv 0 \pmod 2$ and $u > 4$, then there exists an LA(t^u).

Proof. The discussion is divided into two cases, u odd and u even. If u is odd, then t must be even (since tu is even). In this case we just need to consider t = 2 (by Lemma 5.5.2). If u is even, then we consider t = 1.

Case 1: u is odd and t = 2. To construct LA(2^u) we first construct a resolvable 2-GDD(2^u) on N with groups N_k, $1 \le k \le u$. The 2(u - 1) parallel classes are denoted by $\mathcal{P}_h$, $1 \le h \le 2(u - 1)$.

Let $\mathcal{P}_{(2h-1)(2h)} = \mathcal{P}_{2h-1} \cup \mathcal{P}_{2h}$ for $1 \le h \le (u - 1)$. If we view block $\{x, y\}$ as an edge xy, then edges in $\mathcal{P}_{(2h-1)(2h)}$ form disjoint cycles of even edges. Give each cycle an arbitrary direction; then elements of $\mathcal{P}_{(2h-1)(2h)}$ are ordered pairs. Let $\mathcal{Q}_{(2h-1)(2h)} = \{(x, y) : (y, x) \in \mathcal{P}_{(2h-1)(2h)}\}$.

In order to construct 2 anti-symmetric $A(2^u)$, say S_1 and S_2, we construct a 2 by $2(u - 1)$ Latin rectangle L_1 on M. Here we take $M = \{i': 1 \le i \le 2(u - 1)\}$. Its columns are labeled with $\mathcal{P}_{12}$, $\mathcal{Q}_{12}$, $\mathcal{P}_{34}$, $\mathcal{Q}_{34}$, ..., $\mathcal{P}_{(2u-3)(2u-2)}$, $\mathcal{Q}_{(2u-3)(2u-2)}$.

	$\mathcal{P}_{12}$	$\mathcal{Q}_{12}$	$\mathcal{P}_{34}$	$\mathcal{Q}_{34}$	...	$\mathcal{P}_{(2u-5)(2u-4)}$	$\mathcal{Q}_{(2u-5)(2u-4)}$	$\mathcal{P}_{(2u-3)(2u-2)}$	$\mathcal{Q}_{(2u-3)(2u-2)}$
1	1 '	2 '	3 '	4 '	...	(2u - 5) '	(2u - 4) '	(2u - 3) '	(2u - 2) '
2	3 '	4 '	5 '	6 '	...	(2u - 3) '	(2u - 2) '	1 '	2 '

Latin Rectangle L_1

From each row of L_1, we construct two anti-symmetric $A(t^u)$ S_1 and S_2 as follows. $(S_1)(i, j) = (L_1)_{1\mathcal{T}}$ if $(i, j) \in \mathcal{T}$; $(S_2)(i, j) = (L_1)_{2\mathcal{T}}$ if $(i, j) \in \mathcal{T}$, where $\mathcal{T} \in \{\mathcal{P}_{12}, \mathcal{Q}_{12}, \mathcal{P}_{34}, \mathcal{Q}_{34}, ..., \mathcal{P}_{(2u-3)(2u-2)}, \mathcal{Q}_{(2u-3)(2u-2)}\}$.

In order to construct $2(u - 3)$ symmetric $A(t^u)$, S_3, ..., $S_{(u-2)t}$, we first construct a Latin square L_2 of order $2(u - 1)$ on M. Its columns are labeled with $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, $\mathcal{P}_4$, ..., $\mathcal{P}_{2u-3}$, $\mathcal{P}_{2u-2}$. The first 4 rows of L_2 are as follows (L_2 can be viewed as a Latin square extended from the first 4 rows. The extendibility of a Latin rectangle into a Latin square is well known; see, for example, Theorem 3.1 of Chapter 5 in [24]).

	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	$\mathcal{P}_4$	...	$\mathcal{P}_{2u-5}$	$\mathcal{P}_{2u-4}$	$\mathcal{P}_{2u-3}$	$\mathcal{P}_{2u-2}$
1	1 '	2 '	3 '	4 '	...	(2u - 5) '	(2u - 4) '	(2u - 3) '	(2u - 2) '
2	2 '	1 '	4 '	3 '	...	(2u - 4) '	(2u - 5) '	(2u - 2) '	(2u - 3) '
3	3 '	4 '	5 '	6 '	...	(2u - 3) '	(2u - 2) '	1 '	2 '
4	4 '	3 '	6 '	5 '	...	(2u - 2) '	(2u - 3) '	2 '	1 '

The First 4 Rows of Latin Square L_2

From the kth row of L_2, $5 \le k \le 2(u - 1)$, we construct a symmetric $A(2^u)$ S_k as follows. Let $(S_k)(i, j) = (S_k)(j, i) = (L_2)_{k\mathcal{T}}$ if $\{i, j\} \in \mathcal{T}$, where $\mathcal{T} \in \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4, ..., \mathcal{P}_{2u-3}, \mathcal{P}_{2u-2}\}$.

It is not difficult to see that these S_k, $1 \le k \le 2(u - 2)$, form an $LA(t^u)$.

Case 2: u is even and t = 1. An LA(1^6) is presented in the Example of Section 5.2. So we consider u $\geq$ 8. To construct LA(1^u) we first construct a resolvable 2-GDD(1^u) on N with groups N_k, $1 \leq k \leq u$. The u - 1 parallel classes are denoted by $\mathcal{P}_h$, $1 \leq h \leq u - 1$. By Lemma 5.4.1, the resolvable 2-GDD(2^u) on N can have (at least) 3 parallel classes, say $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, whose union is a bipartite graph. Let $\mathcal{P}_{12} = \mathcal{P}_1 \cup \mathcal{P}_2$, $\mathcal{P}_{23} = \mathcal{P}_2 \cup \mathcal{P}_3$ and $\mathcal{P}_{31} = \mathcal{P}_3 \cup \mathcal{P}_1$. As before we view pair {x, y} as an edge xy. Edges in $\mathcal{P}_{12}$ (or $\mathcal{P}_{23}$, $\mathcal{P}_{31}$) form disjoint cycles of even edges. Give each cycle in $\mathcal{P}_{12}$ an arbitrary direction. Then assign direction to cycles of $\mathcal{P}_{23}$ and $\mathcal{P}_{31}$, such that

for $\{x, y\} \in \mathcal{P}_2$ and $(x, y) \in \mathcal{P}_1 \cup \mathcal{P}_2$, $(y, x) \in \mathcal{P}_{23}$,
for $\{x, y\} \in \mathcal{P}_1$ and $(x, y) \in \mathcal{P}_1 \cup \mathcal{P}_2$, $(y, x) \in \mathcal{P}_{31}$.

Since $\mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3$ is a bipartite graph, the above requirement is available and the following condition is satisfied:

for $\{x, y\} \in \mathcal{P}_3$, $(x, y) \in \mathcal{P}_{23}$ if and only if $(y, x) \in \mathcal{P}_{31}$.

Let $\mathcal{P}_{(2h)(2h+1)} = \mathcal{P}_{2h} \cup \mathcal{P}_{2h+1}$ for $2 \leq h \leq (u - 2) / 2$. Give each cycle of $\mathcal{P}_{(2h)(2h+1)}$ an arbitrary direction and let $Q_{(2h)(2h+1)} = \{(x, y) : (y, x) \in \mathcal{P}_{(2h)(2h+1)}\}$ for $2 \leq h \leq (u - 2) / 2$.

In order to construct one anti-symmetric A(t^u), say S_1, we construct a 1 by u - 1 Latin rectangle L_3 on M (here we take $M = \{i': 1 \leq i \leq u - 1\}$). Its columns are labeled with $\mathcal{P}_{12}$, $\mathcal{P}_{23}$, $\mathcal{P}_{31}$, $\mathcal{P}_{45}$, Q_{45}, $\mathcal{P}_{67}$, Q_{67}, ..., $\mathcal{P}_{(u-2)(u-1)}$, $Q_{(u-2)(u-1)}$.

	$\mathcal{P}_{12}$	$\mathcal{P}_{23}$	$\mathcal{P}_{31}$	$\mathcal{P}_{45}$	Q_{45}	$\mathcal{P}_{67}$	Q_{67}	...	$\mathcal{P}_{(u-2)(u-1)}$	$Q_{(u-2)(u-1)}$
1	1'	2'	3'	4'	5'	6'	7'	...	(u - 2)'	(u - 1)'

Latin Rectangle L_3

From the only row of L_3, we construct an anti-symmetric A(1^u) S_1 as follows. Let $(S_1)(i, j) = (L_3)_{1T}$ if $(i, j) \in \mathcal{T}$, where $\mathcal{T} \in \{\mathcal{P}_{12}, \mathcal{P}_{23}, \mathcal{P}_{31}, \mathcal{P}_{45}, Q_{45}, \mathcal{P}_{67}, Q_{67}, ..., \mathcal{P}_{(u-2)(u-1)}, Q_{(u-2)(u-1)}\}$

In order to construct u - 3 symmetric A(1^u), S_2,..., S_{u-2}, we first construct a Latin square L_4 of order u - 1 on M. Its columns are labeled with $\mathcal{P}_1$, $\mathcal{P}_2$, ..., $\mathcal{P}_{u-2}$, $\mathcal{P}_{u-1}$. The first 2 rows of L_4

are as follows. L_4 can be viewed as a Latin square extended from the first 2 rows (a Latin rectangle).

	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	$\mathcal{P}_4$	$\mathcal{P}_5$	$\mathcal{P}_6$	$\mathcal{P}_7$	...	$\mathcal{P}_{u-2}$	$\mathcal{P}_{u-1}$
1	1 '	2 '	3 '	4 '	5 '	6 '	7 '		(u - 2) '	(u - 1) '
2	3 '	1 '	2 '	5 '	4 '	7 '	6 '	...	(u - 1) '	(u - 2) '

The First 2 Rows of Latin Square L_4

From the kth row of L_4, $3 \le k \le u - 2$, we construct a symmetric $A(1^u)$ S_k as follows. Let $(S_k)(i, j) = (S_k)(j, i) = (L_4)_{k\mathcal{T}}$ if $\{i, j\} \in \mathcal{T}$, where $\mathcal{T} \in \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{u-2}, \mathcal{P}_{u-1}\}$.

It is verified that these S_k, $1 \le k \le u - 2$, form a $LA(1^u)$. This completes our proof. ♦

Lemma 5.5.5 There exists an $LA(1^u)$ associated with a resolvable 2-$GDD(1^u)$ for even $u \ge 6$.

Proof. If an $LA(1^u)$ exists, then any resolvable 2-$GDD(1^u)$ will associated with this $LA(1^u)$. The result then follows from Lemma 5.5.4. ♦

For odd $u \ge 5$, although an $LA(2^u)$ exists by Lemma 5.5.4, we have not succeeded in constructing an $LA(2^u)$ associated with a resolvable 2-$GDD(2^u)$.

5.6 Summary of this chapter

Theorem 5.6.1 (Rosa's Theorem) Suppose $u \ge 4$ is even and $t \in \{3, 6\}$. If an $LSDG(t^{u-1})$ exists, then there exists an $LSDG(t^{2u-1})$.

Proof. An H(u, t, 4, 3) exists for all even $u \ge 4$ by Lemma 5.2.1. There is an $LA(1^u)$ associated with a resolvable 2-$GDD(1^u)$ for even $u \ge 6$ by Lemma 5.5.5. There is also an $LA(3^4)$ associated with a resolvable 2-$GDD(3^4)$ by Lemma 5.5.3. So there is an $LA(t^u)$ associated with a resolvable 2-$GDD(t^u)$ by Lemma 5.5.2 for $t \in \{3, 6\}$ and even $u \ge 4$. Therefore, by Lemma 5.3.4, we have an $LSDG(t^{2u-1})$ from an $LSDG(t^{u-1})$. ♦

Chapter 6

Another Tripling Construction

Main Results

1. Suppose $n \geq 3$. Suppose an n-AD(t, v) and an LD(v) exist. If there exists an LSDG($t^3(nt\text{-}2t)^1$), then there exists an LSDG($t^{3v}(nt\text{-}2t)^1$).

2. Suppose $v \equiv 1 \pmod 6$. If there exists an LSDP(v+4), then an LSDP(7v+4) exists.

6.1 Introduction

In this chapter, we introduce an auxiliary design to help us establish a recursive construction. Section 6.2 discusses LD(v) introduced by Lu ([20]) which will be used in section 6.4. Section 6.3 introduces the auxiliary design n-AD(t, v). Section 6.4 uses n-AD(t, v) to establish a "tripling" recursive construction for large sets of disjoint 3-GDDs. Section 6.5 gives a useful recursive construction for 4-AD(1, v). Section 6.6 constructs some small 4-AD(1, v). Results of this chapter are presented in section 6.7. Material in sections 6.5 and 6.6 has been published in [4].

6.2 Preliminaries

A *pairwise balanced design* (PBD) is a pair (X, $\mathcal{B}$), where X is a finite set of points and $\mathcal{B}$ is a set of subsets of X called *blocks*, such that every pair of elements of X appears in a unique block. Suppose K is a set of integers. Define B[K] to be the set of v such that there exists a PBD (X, $\mathcal{B}$), where X is of size v and the sizes of blocks in $\mathcal{B}$ are in K. K is said to be *PBD-closed* if B[K] = K.

A *transversal design* TD(k, v) is a k-GDD(v^k). If we view groups in a GDD as among the blocks, a GDD is a PBD. Particularly, if a TD(k, v) exists, then $kv \in B[k, v]$.

Suppose V is a set of size v. An *orthogonal array* $\mathcal{L}$, denoted by OA(2, k, v), is a set of v^2 ordered k-tuples such that, for any 2-subset {i, j} of {1, 2, ..., k} and for two arbitrary elements x_1 and x_2 of V (not necessary distinct), there is a unique element $(y_1, ..., y_k)$ of $\mathcal{L}$ with $y_i = x_1$ and $y_j = x_2$. It is well known that an OA(2, k, v) is equivalent to a TD(k, v).

An LD(v) on V is a set $\{\mathcal{L}^1, \mathcal{L}^2\} \cup \{\mathcal{L}_x: x \in V\}$ satisfying the following conditions:

(6.2.1) $\mathcal{L}_x$ is an OA(2, 3, v - 1) on $V \setminus \{x\}$, for $x \in V$.

(6.2.2) $\mathcal{L}^j$ is an OA(2, 4, v) on V, for $j = 1, 2$.

(6.2.3) $\exists\, x' \in V$ such that $(x, x, x, x') \in \mathcal{L}^1 \cap \mathcal{L}^2$, for all $x \in V$.

(6.2.4) Any $(x_1, x_2, x_3) \in V^3$ is either in $\mathcal{L}_x$, for some $x \in V$, or in $\mathcal{L}^{1*}$ or in $\mathcal{L}^{2*}$, where $\mathcal{L}^{j*}=\{(x_1, x_2, x_3) : \exists\, x \in V$ such that $(x_1, x_2, x_3, x) \in \mathcal{L}^j\}$ for $j = 1, 2$.

An LD*(v) on V is an LD(v) satisfying one more condition

(6.2.5) $\mathcal{L}= \{(x_0, x_1, x_2, x_3) : (x_0, x_2, x_3) \subseteq A \in \mathcal{L}^1, (x_1, x_2, x_3) \subseteq B \in \mathcal{L}^2\}$ is an OA(2, 4, v).

An LD^i(v) on V is defined in the same way as LD(v), except (6.2.3) in the above definition is changed into

(6.2.3') for all $x \in V$, $(x, x, x, x) \in \mathcal{L}^1 \cap \mathcal{L}^2$.

LD(v) and LD*(v) were introduced and used by Lu ([20]) to construct large sets of disjoint Steiner triple systems. LD^i(v) was defined by Teirlinck ([30]) to prove that the set {v : both an LD(v) and an LD^i(v) exist} is PBD-closed. It was also proved that the existence of an LD*(v) implies the existence of an LD^i(v). In [30], it was proved that {v : LD*(v) exists} is PBD-closed. The following result is quoted from [17]. An LD(v) exists for $v \geq 4$ and $v \neq 6$, except possibly for v = 9, 10, 14, 18, 23, 26, 27, 30, 38, 42, 46, 62, 74, 86, 90 and 114. An LD*(v) exists for $v \geq 4$ and $v \neq 6$, except possibly for v = 9, 10, 12, 14, 15 18, 23, 26, 27, 30, 38, 42, 46, 62, 66, 74, 86, 90 and 114.

Now we eliminate seven of the sixteen possible exceptions for LD(v). First we construct an LD*(9) on $V = GF(3^2)$, the finite field with primitive polynomial $\xi^2 + 2\xi + 2$. LD*(9) will be $\{\mathcal{L}^1, \mathcal{L}^2\} \cup \{\mathcal{L}_x: x \in V\}$. $\mathcal{L}_x$, $x \in V$, are developed from $\mathcal{L}_0$, i.e., if $(x_1, x_2, x_3) \in \mathcal{L}_0$,

then $(x_1 + x, x_2 + x, x_3 + x) \in \mathcal{L}_x$. We display $\mathcal{L}_0$, $\mathcal{L}^1$, $\mathcal{L}^2$. In the following, $(x_1, x_2, x_3)\xi^i$ means $(x_1 \xi^i, x_2 \xi^i, x_3 \xi^i)$. $\mathcal{L}_0$ consists of the following 64 ordered triples:

$(1, \xi^4, 1)\,\xi^{2i}$	$(\xi, 1, \xi)\,\xi^{2i}$	$(1, \xi^7, \xi^7)\,\xi^{2i}$	$(\xi, \xi^6, \xi^6)\,\xi^{2i}$
$(\xi, \xi^4, \xi^3)\,\xi^{2i}$	$(1, \xi^6, \xi)\,\xi^{2i}$	$(\xi, \xi^7, \xi^4)\,\xi^{2i}$	$(1, \xi, \xi^2)\,\xi^{2i}$
$(1, \xi^5, \xi^3)\,\xi^{2i}$	$(1, \xi^2, \xi^4)\,\xi^{2i}$	$(\xi, \xi^2, 1)\,\xi^{2i}$	$(\xi, \xi^5, \xi^7)\,\xi^{2i}$
$(x, \xi^3, \xi^2)\,\xi^{2i}$	$(1, \xi^3, \xi^6)\,\xi^{2i}$	$(1, 1, \xi^5)\,\xi^{2i}$	$(\xi, \xi, \xi^5)\,\xi^{2i}$

where $0 \le i \le 3$.

$\mathcal{L}^1 = \{(x + t, \xi^2 x + t, \xi^7 x + t, x) : x, t \in V\}$.
$\mathcal{L}^2 = \{(x + t, \xi^2 x + t, \xi^5 x + t, x) : x, t \in V\}$.

Since an LD*(v) exists for $v \in \{4, 5, 7, 8, 11, 16\}$, an LD*(v) exists for $v \in B[4, 5, 7, 8, 9, 11, 16]$. Take a (transversal design) TD(9, 16) and select two groups. By deleting 15 points from each of the two groups, we have $114 \in B[7, 8, 9, 16]$. Hence an LD*(114) exists. Take a TD(9, 11) and select two groups. Delete 3 points from one group, 6 points from another; then we have $90 \in B[5, 7, 8, 9, 11]$. Hence an LD*(90) exists. Take a TD(8, 11) and delete 2 point from a group; then we have $86 \in B[7, 8, 9, 11]$. Hence an LD*(86) exists. Take a TD(9, 9) and select two groups. Delete 2 points from one group, 5 points from another; then we have $74 \in B[4, 7, 8, 9]$. Hence an LD*(74) exists. Take a TD(9, 8) and select two groups. Delete 3 points from one group, 7 points from another; then we have $62 \in B[5, 7, 8, 9]$. Hence an LD*(62) exists. Since an LD*(9) (hence an LD(9)) exists, an LD(27) exists (by [14]). The result is summarized in the following.

Lemma 6.2.1 An LD(v) exists for $v \ge 4$ and $v \ne 6$, except possibly for v = 10, 14, 18, 23, 26, 30, 38, 42 and 46.

6.3 The auxiliary design

Let X be a set of size $v \equiv 1$ or 3 (mod 6), $v > 7$. Suppose a and b are two elements of X. Suppose Steiner triple systems $(X, \mathcal{B}_i)$, $1 \le i \le v - 2$, form a large set. Delete the block which contains both a and b from each $\mathcal{B}_i$, $1 \le i \le v - 2$. Then we end up with a set of disjoint 3-GDD($1^{v-3}3^1$). These 3-GDD($1^{v-3}3^1$) do not have the same group set. We will generalize them into a kind of auxiliary design as follows.

Let V be a set of size v. Suppose S is a set of size tv, and Ω is a set of size tn which is disjoint from S. Let $\{G_x : x \in V\}$ be a partition of S into subsets of size t. For $x \in V$, let $\mathcal{G}_x$ consist of G_y ($y \in V \setminus \{x\}$) and $\Omega \cup G_x$.

Let $X = S \cup \Omega$. Let $n \geq 2$. An *auxiliary design*, denoted by n-AD(t, v), is a set consisting of $(X, \mathcal{G}_x, \mathcal{A}_s)$ ($x \in V$, $s \in G_x$) and $(S, \mathcal{B}_k)$ ($0 \leq k < t(n - 2)$) such that

(6.3.1) $(X, \mathcal{G}_x, \mathcal{A}_s)$ ($x \in V$, $s \in G_x$) are 3-GDD($t^{v-1}(tn+t)^1$),

(6.3.2) $(S, \mathcal{B}_k)$ ($0 \leq k < t(n - 2)$) are 3-GDD(t^v),

(6.3.3) $\mathcal{A}_s$ ($x \in V$, $s \in G_x$) and $\mathcal{B}_k$ ($0 \leq k < t(n - 2)$) are mutually disjoint.

From the necessary conditions for the existence of a 3-GDD($t^{v-1}(tn+t)^1$) and of a 3-GDD(t^v), we have the necessary conditions for the existence of an n-AD(t, v):

$v \geq n + 3$,
$tn \equiv 0 \pmod 2$,
$t(v + n - 1) \equiv 0 \pmod 2$,
$t^2(v - 1)(v + 2n) \equiv 0 \pmod 6$,
if $t(n - 2) \geq 1$, then $t^2v(v - 1) \equiv 0 \pmod 6$.

An immediate and easy construction is the following.

Lemma 6.3.1 If an n-AD(t, v) exists, then there is an n-AD(tw, v) for $w > 0$.

Proof. Suppose V, S, Ω, $\{G_x : x \in V\}$ and $\mathcal{G}_x$ are defined as before. Let $X = S \cup \Omega$. Take an n-AD(t, v) on X consisting of $(X, \mathcal{G}_x, \mathcal{A}_s)$ ($x \in V$, $s \in G_x$) and $(S, \mathcal{B}_k)$ ($0 \leq k < t(n - 2)$).

Let $X' = (S \cup \Omega) \times Z_w$. Now we construct on X' an n-AD(tw, v) consisting of $(X', \mathcal{G}_x', \mathcal{A}_s')$ ($x \in V$, $s \in G_x'$) and $(S', \mathcal{B}_k')$ ($0 \leq k < tw(n - 2)$). The definitions are as follows. $S' = S \times Z_w$, $\Omega' = \Omega \times Z_w$, $G_x' = G_x \times Z_w$. For $x \in V$, let $\mathcal{G}_x'$ consist of G_y' ($y \in V \setminus \{x\}$) and $\Omega' \cup G_x'$. For $s = (r, i)$, $r \in G_x$ and $i \in Z_w$, $\mathcal{A}_s' = \{ \{(x, a), (y, b), (z, c)\} : \{x, y, x\} \in \mathcal{A}_r$ and $a + b + c \equiv i \pmod w\}$. For k, $0 \leq k < tw(n - 2)$, $\mathcal{B}_k' = \{\{(x, a), (y, b), (z, c)\} : \{x, y, x\} \in \mathcal{B}_r$, where $r = k \pmod{t(n - 2)}$, and $a + b + c \equiv k \pmod w\}$. Thus an n-AD(tw, v) is constructed. ♦

A 2-AD(t, v) is just a set of tv disjoint 3-GDD($t^{v-1}(3t)^1$). A 3-GDD($t^{v-1}(3t)^1$) can be used to get a 3-GDD(t^{v+2}). Therefore, we have the following.

Lemma 6.3.2 If a 2-AD(t, v) exists, then there is an LSDG(t^{v+2}).

Among the most interesting auxiliary designs is 4-AD(1, v). The necessary condition for the existence of a 4-AD(1, v) is $v \equiv 1 \pmod 6$ and $v \geq 7$.

Lemma 6.3.3 If a 4-AD(1, v) exists, then there is an LSDP(v+4).

Proof. Let V be a set of size v. Suppose a 4-AD(1, v), consisting of $(X, \mathcal{G}_x, \mathcal{A}_s)$ ($x \in V$, $s \in G_x$) and $(S, \mathcal{B}_k)$ ($0 \leq k < 2$), is given on point set $X = S \cup \Omega$, where $S = Z_v$, $\Omega = \{\infty_1, \infty_2, \infty_3, \infty_4\}$, $G_x = \{x - 1\}$, $x \in V$, and $\mathcal{G}_x$ consists of G_y ($y \in V \setminus \{x\}$) and $\Omega \cup G_x$.

For each $(X, \mathcal{G}_x, \mathcal{A}_s)$ ($x \in V$, $s \in G_x$), we construct a (2, 3)-packing $(X, \mathcal{C}_x)$ as follows. $\mathcal{C}_x$ consists of the blocks in $\mathcal{A}_s$ and two more : $\{\infty_1, \infty_3, x - 1\}$ and $\{\infty_2, \infty_4, x - 1\}$. Then the leave of the (2, 3)-packing is a 4-cycle $\{\{\infty_1, \infty_2\}, \{\infty_2, \infty_3\}, \{\infty_3, \infty_4\}, \{\infty_4, \infty_1\}\}$. Therefore, $(X, \mathcal{C}_x)$ ($x \in V$) form a LSDP(v+4). ♦

The above lemmas are not the only ones that make auxiliary designs useful. In the next section we present another use of auxiliary designs. Section 6.5 will give some more 4-AD(1, v) by recursive construction.

6.4 The use of the auxiliary design

Lemma 6.4.1 Suppose $n \geq 3$. Suppose an n-AD(t, v) and an LD(v) exist. If there exists an LSDG($t^3(nt-2t)^1$), then there exists an LSDG($t^{3v}(nt-2t)^1$).

Proof. Let V be a set of size v. Take an LD(v) on V which consists of $\mathcal{L}^1$, $\mathcal{L}^2$, and $\mathcal{L}_x$ ($x \in V$). Let $S = Z_t \times V$. Suppose Ω is a set of size tn. $S \cap \Omega = \varnothing$. The partition of S is $\{G_x : x \in V\}$, where $G_x = Z_t \times \{x\}$. Let $\mathcal{G}_x$ consist of G_y ($y \in V \setminus \{x\}$) and $\Omega \cup G_x$. Take an n-AD(t, v) on $S \cup \Omega$, consisting of $(S \cup \Omega, \mathcal{G}_x, \mathcal{A}_s)$ ($x \in V$, $s \in G_x$), which are 3-GDD($t^{v-1}(tn+t)^1$), and $(S, \mathcal{B}_k)$ ($0 \leq k < t(n - 2)$), which are 3-GDD(t^v).

We will construct 3-GDD($t^{3v}(nt-2t)^1$) on point set

$$X = (S \times Z_3) \cup \Gamma,$$

where Γ is a set of size t(n-2) and disjoint from $S \times Z_3$. The groups $\mathcal{G}$ will consist of

$$Z_t \times \{(x, j)\} \ ((x, j) \in V \times Z_3) \text{ and } \Gamma.$$

The block sets are constructed using three methods, which will produce tv, t and tv - 2t block sets respectively. These block sets will form an LSDG($t^3v(nt-2t)^1$).

Method one

In this method, we make use of $\mathcal{L}_x$ ($x \in V$) and ($S \cup \Omega$, $\mathcal{G}_x$, $\mathcal{A}_s$) in the constructed n-AD(t, v) ($x \in V$, $s \in G_x$).

For $x \in V$, do the following.

1) If $(x_0, x_1, x_2) \in \mathcal{L}_x$, then construct an LSDG(t^3), with groups $Z_t \times \{(x_0, 0)\}$, $Z_t \times \{(x_1, 1)\}$ and $Z_t \times \{(x_2, 2)\}$. Name the block sets $(x_0,x_1,x_2)_s$, $s \in G_x$. Let $\mathcal{L}_x_s = \cup (x_0,x_1,x_2)_s$, where the union is done for all $(x_0, x_1, x_2) \in \mathcal{L}_x$.

2) For $j \in Z_3$, take a 1-1 mapping ψ_j from $S \cup \Omega$ to $(S \times \{j\}) \cup (\Gamma \cup \Psi)$, where $\Psi = Z_t \times \{x\} \times (Z_3 \setminus \{j\})$, such that $\psi_j(r) = (r, j)$ for $r \in S$. Let $\psi_j(\mathcal{A}_s) = \{\psi_j A : A \in \mathcal{A}_s\}$, for $s \in G_x$, $j \in Z_3$.

3) Take an LSDG($t^3(nt-2t)^1$), which exists by the assumption, with groups $Z_t \times \{(x, j)\}$ ($j \in Z_3$) and Γ. Name the 2t block sets $\mathcal{C}_{sm}$ ($s \in G_x$, m=0, 1). ($\mathcal{C}_{s0}$ ($s \in G_x$) will be used up in this method. The other t block sets $\mathcal{C}_{s1}$ ($s \in G_x$) are saved for use in Method two.)

Then, let

$$\mathcal{D}_{xs} = \mathcal{L}_x_s \cup \psi_0(\mathcal{A}_s) \cup \psi_1(\mathcal{A}_s) \cup \psi_2(\mathcal{A}_s) \cup \mathcal{C}_{s0},$$

where $x \in V$ and $s \in G_x$. We claim that $(X, \mathcal{G}, \mathcal{D}_{xs})$ are 3-GDD($t^3v(nt-2t)^1$).

Method two

This method uses $\mathcal{L}^1$ and $(S, \mathcal{B}_k)$ in the constructed n-AD(t, v), where $0 \le k < t(n-2)$. Recall that $\mathcal{L}^{1*} = \{(x_1, x_2, x_3) :$ there is an $x \in V$ such that $(x_1, x_2, x_3, x) \in \mathcal{L}^1\}$. $\mathcal{L}^{1*}$ is an OA(2, 3, v). We do the following.

1) If $(x_0, x_1, x_2) \in \mathcal{L}^{1*}$ and $x_0 \neq x_1 \neq x_2 \neq x_0$, then construct an LSDG(t^3), with groups $Z_t \times \{(x_0, 0)\}$, $Z_t \times \{(x_1, 1)\}$ and $Z_t \times \{(x_2, 2)\}$. The block sets are denoted by $(x_0,x_1,x_2)_i$, $i \in Z_t$. Let $\mathcal{L}^{1*}_i = \{(x_0,x_1,x_2)_i : (x_0, x_1, x_2) \in \mathcal{L}^{1*}$ and $x_0 \neq x_1 \neq x_2 \neq x_0\}$, $i \in Z_t$.

2) For $j \in Z_3$, take the same 1-1 mapping ψ_j as in part 2) of Method one, but restrict it on S to $S \times \{j\}$. Let $\psi_j(\mathcal{B}_i) = \{\{\psi_j B : B \in \mathcal{B}_i\}$, for $i \in Z_t$, $j \in Z_3$. (If $n>3$, $\mathcal{B}_k$ with $k \ge t$ has not been used and will never be used.)

Then let

$$\mathcal{E}_i = \mathcal{L}^{1*}_i \cup \psi_0(\mathcal{B}_i) \cup \psi_1(\mathcal{B}_i) \cup \psi_2(\mathcal{B}_i) \cup (\bigcup_{x \in V} C_{s1}),$$

where $s = (i, x) \in G_x$, $i \in Z_t$. We claim that $(X, \mathcal{G}, \mathcal{E}_i)$ $(i \in Z_t)$ are 3-GDD($t^{3v}(nt-2t)^1$). (Note that $\mathcal{B}_i$ $(i \ge t)$ are not been used and will never be used.)

Method three

This method mainly uses $\mathcal{L}^2$. Suppose $x' \in V$ such that $(x, x, x, x') \in \mathcal{L}^2$. We need some preparation here. Choose a t-subset of Ω : $\Lambda = \{\alpha_k : k \in Z_t\}$. For $s \in G_x$, from $(S \cup \Omega, \mathcal{G}_x, \mathcal{A}_s)$ we define a set of pairs as follows. $\mathcal{P}_{sk} = \{\{(i_0, y_0), (i_1, y_1)\} : \{(i_0, y_0), (i_1, y_1), \alpha_k\} \in \mathcal{A}_s\}$. So, for $s \in G_x$, $\mathcal{P}_{sk}$ is a partition of $S \setminus G_x$. Now, for $x \in V \setminus \{x'\}$, do the following.

1) If $(x_0, x_1, x_2, x) \in \mathcal{L}^2$, construct an LSDG($t^3(nt-2t)^1$), with groups $Z_t \times \{(x_0, 0)\}$, $Z_t \times \{(x_1, 1)\}$, $Z_t \times \{(x_2, 2)\}$ and Γ. Name the 2t block sets as $(x_0, x_1, x_2, x)_sm$, $s \in G_x$, $m = 0, 1$. Let $\mathcal{L}^2_{sm} = \cup (x_0, x_1, x_2, x)_sm$, $s \in G_x$, $m = 0, 1$, where the union is done for all $(x_0, x_1, x_2, x) \in \mathcal{L}^2$.

2) For $s \in G_x$, if $(x_0, x_1, x_2, x) \in \mathcal{L}^2$, let $\mathcal{F}_{s0}$ consist of the following blocks :

$\{(k, x_0, 0), (i_0, y_0, 1), (i_1, y_1, 1)\}$ for $\{(i_0, y_0), (i_1, y_1)\} \in \mathcal{P}_{s_1 k}$, $k \in Z_t$, where $s_1 = (i, x_1)$;

$\{(k, x_1, 1), (i_0, y_0, 2), (i_1, y_1, 2)\}$ for $\{(i_0, y_0), (i_1, y_1)\} \in \mathcal{P}_{s_2k}$, $k \in Z_t$, where $s_2 = (i, x_2)$;
$\{(k, x_2, 2), (i_0, y_0, 0), (i_1, y_1, 0)\}$ for $\{(i_0, y_0), (i_1, y_1)\} \in \mathcal{P}_{s_0k}$, $k \in Z_t$, where $s_0 = (i, x_0)$.

Let $\mathcal{F}_{s1}$ consist of the following blocks :

$\{(k, x_0, 0), (i_0, y_0, 2), (i_1, y_1, 2)\}$ for $\{(i_0, y_0), (i_1, y_1)\} \in \mathcal{P}_{s_2k}$, $k \in Z_t$, where $s_2 = (i, x_2)$;
$\{(k, x_1, 1), (i_0, y_0, 0), (i_1, y_1, 0)\}$ for $\{(i_0, y_0), (i_1, y_1)\} \in \mathcal{P}_{s_0k}$, $k \in Z_t$, where $s_0 = (i, x_0)$;
$\{(k, x_2, 2), (i_0, y_0, 1), (i_1, y_1, 1)\}$ for $\{(i_0, y_0), (i_1, y_1)\} \in \mathcal{P}_{s_1k}$, $k \in Z_t$, where $s_1 = (i, x_1)$;

Let

$$\mathcal{H}_{sm} = \mathcal{L}^2_{sm} \cup \mathcal{F}_{sm},$$

$s \in G_x$, $x \in V \setminus \{x'\}$, $m = 0, 1$. We claim that $(X, \mathcal{G}, \mathcal{H}_{sm})$ are 3-GDD$(t^{3v}(nt-2t)^1)$.

The three methods together give an LSDG$(t^{3v}(nt-2t)^1)$. ◆

6.5 Construction for 4-AD(1, v)

First, we present a result which will be used subsequently.

Lemma 6.5.1 Suppose $v \equiv 1 \pmod 6$. There exists an LSDG(v^3) in which each 3-GDD has a parallel class and these v parallel classes form the block set of 3-GDD of type v^3.

Proof. Let $S = \{a, b, c\}$. Let $X = S \times Z_V$ and $\mathcal{G} = \{\{s\} \times Z_V : s \in S\}$. For every $i \in Z_V$, let $\mathcal{B}_i = \{\{(a, x), (b, y), (c, z)\} : x + y + z \equiv 3i \pmod v\}$. Then $(X, \mathcal{G}, \mathcal{B}_i)$, $i \in Z_V$, form v disjoint 3-GDDs. Therefore they form an LSDG(v^3). Let $\mathcal{P}_i = \{\{(a, x + i), (b, 2x + i), (c, -3x + i)\} : x \in Z_V\}$. Then each $\mathcal{P}_i$ is a parallel class in $\mathcal{B}_i$, and $(X, \mathcal{G}, \cup_{1 \le i \le v}\mathcal{P}_i)$ is a 3-GDD of type v^3. ◆

Now we present a construction of a 4-AD(1, 7v) from a 4-AD(1, v), where $v \equiv 1 \pmod 6$.

In [25], a set of 7 disjoint compatible packings on 11 points (i.e., an LSDP(11)) was presented. It can be modified to give a 4-AD(1, 7) with some special and useful properties. The 4-AD(1, 7) consists of $(X, \mathcal{G}_i, \mathcal{A}_i)$ $(1 \le i \le 7)$ and $(X, \mathcal{B}_k)$ $(0 \le k < 2)$, where the point set

$X = Z_7 \cup \Omega$, $\Omega = \{\infty_1, \infty_2, \infty_3, \infty_4\}$, $G_i = \{i - 1\}$, $1 \le i \le 7$, and $\mathcal{G}_i$ consists of G_j ($1 \le j \le 7$, $j \ne i$) and $\Omega \cup G_i$. We list $\mathcal{A}_i$ in Table 6.5.1 and classify the blocks of each $\mathcal{A}_i$, into 3 types. $\mathcal{B}_k$ are listed in Table 6.5.2.

	$\mathcal{A}_1$:	$\mathcal{A}_2$:	$\mathcal{A}_3$:	$\mathcal{A}_4$:	$\mathcal{A}_5$:	$\mathcal{A}_6$:	$\mathcal{A}_7$:
type 1:	$\{\infty_1, 4, 6\}$	$\{\infty_2, 5, 0\}$	$\{\infty_4, 6, 1\}$	$\{\infty_3, 0, 2\}$	$\{\infty_4, 1, 3\}$	$\{\infty_2, 2, 4\}$	$\{\infty_3, 3, 5\}$
	$\{\infty_2, 6, 2\}$	$\{\infty_1, 0, 3\}$	$\{\infty_2, 1, 4\}$	$\{\infty_4, 2, 5\}$	$\{\infty_3, 3, 6\}$	$\{\infty_3, 4, 0\}$	$\{\infty_2, 5, 1\}$
	$\{\infty_3, 2, 3\}$	$\{\infty_3, 3, 4\}$	$\{\infty_1, 4, 5\}$	$\{\infty_2, 5, 6\}$	$\{\infty_1, 6, 0\}$	$\{\infty_2, 0, 1\}$	$\{\infty_4, 1, 2\}$
	$\{\infty_2, 3, 1\}$	$\{\infty_1, 4, 2\}$	$\{\infty_2, 5, 3\}$	$\{\infty_4, 6, 4\}$	$\{\infty_3, 0, 5\}$	$\{\infty_1, 1, 6\}$	$\{\infty_2, 2, 0\}$
	$\{\infty_4, 1, 5\}$	$\{\infty_4, 2, 6\}$	$\{\infty_3, 3, 0\}$	$\{\infty_1, 4, 1\}$	$\{\infty_2, 5, 2\}$	$\{\infty_2, 6, 3\}$	$\{\infty_1, 0, 4\}$
	$\{\infty_2, 5, 4\}$	$\{\infty_1, 6, 5\}$	$\{\infty_2, 0, 6\}$	$\{\infty_4, 1, 0\}$	$\{\infty_3, 2, 1\}$	$\{\infty_4, 3, 2\}$	$\{\infty_2, 4, 3\}$
type 2:	$\{\infty_1, 1, 2\}$	$\{\infty_2, 2, 3\}$	$\{\infty_4, 3, 4\}$	$\{\infty_3, 4, 5\}$	$\{\infty_4, 5, 6\}$	$\{\infty_4, 6, 0\}$	$\{\infty_3, 0, 1\}$
	$\{\infty_4, 2, 4\}$	$\{\infty_4, 3, 5\}$	$\{\infty_3, 4, 6\}$	$\{\infty_1, 5, 0\}$	$\{\infty_2, 6, 1\}$	$\{\infty_1, 0, 2\}$	$\{\infty_1, 1, 3\}$
	$\{\infty_3, 4, 1\}$	$\{\infty_3, 5, 2\}$	$\{\infty_1, 6, 3\}$	$\{\infty_2, 0, 4\}$	$\{\infty_1, 1, 5\}$	$\{\infty_3, 2, 6\}$	$\{\infty_4, 3, 0\}$
	$\{\infty_1, 3, 5\}$	$\{\infty_2, 4, 6\}$	$\{\infty_4, 5, 0\}$	$\{\infty_3, 6, 1\}$	$\{\infty_4, 0, 2\}$	$\{\infty_3, 1, 3\}$	$\{\infty_3, 2, 4\}$
	$\{\infty_3, 5, 6\}$	$\{\infty_3, 6, 0\}$	$\{\infty_1, 0, 1\}$	$\{\infty_2, 1, 2\}$	$\{\infty_1, 2, 3\}$	$\{\infty_1, 3, 4\}$	$\{\infty_4, 4, 5\}$
	$\{\infty_4, 6, 3\}$	$\{\infty_4, 0, 4\}$	$\{\infty_3, 1, 5\}$	$\{\infty_1, 2, 6\}$	$\{\infty_2, 3, 0\}$	$\{\infty_4, 4, 1\}$	$\{\infty_1, 5, 2\}$
type 3:	{0, 1, 6}	{1, 2, 0}	{2, 3, 1}	{3, 4, 2}	{4, 5, 3}	{5, 6, 4}	{6, 0, 5}
	{0, 2, 5}	{1, 3, 6}	{2, 4, 0}	{3, 5, 1}	{4, 6, 2}	{5, 0, 3}	{6, 1, 4}
	{0, 3, 4}	{1, 4, 5}	{2, 5, 6}	{3, 6, 0}	{4, 0, 1}	{5, 1, 2}	{6, 2, 3}

Table 6.5.1

$\mathcal{B}_0$	{1, 2, 4}	{2, 3, 5}	{3, 4, 6}	{4, 5, 0}	{5, 6, 1}	{6, 0, 2}	{0, 1, 3}
$\mathcal{B}_1$	{3, 5, 6}	{4, 6, 0}	{5, 0, 1}	{6, 1, 2}	{0, 2, 3}	{1, 3, 4}	{2, 4, 5}

Table 6.5.2

For $1 \le k \le 3$, define $\mathcal{A}_{ik}$ to be the set of blocks of type k in $\mathcal{A}_i$. The following properties will be important in our construction.

(6.5.1) For $x \in \{\infty_1, \infty_2, \infty_3, \infty_4\}$, define $E_i(2, x) = \{\{a, b\}: \{x, a, b\} \in \mathcal{A}_{i1}\}$. Then $E_i(2) = \cup_{x \in \{\infty 1, \infty 2, \infty 3, \infty 4\}} E_i(2, x)$ forms a 6-cycle on $Z_7 \setminus \{i - 1\}$. Direct edges in $E_i(2)$ so that every point has indegree one and outdegree one, and call the resulting collection of ordered pairs $D_i(2)$. Then the ordered

pairs $D_i(2)$, $1 \le i \le 7$, can be arranged so that they are mutually disjoint. For example, this can be done as follows.

$D_1(2)$:	$D_2(2)$:	$D_3(2)$:	$D_4(2)$:	$D_5(2)$:	$D_6(2)$:	$D_7(2)$:
(4, 6)	(5, 0)	(6, 1)	(0, 2)	(1, 3)	(2, 4)	(3, 5)
(6, 2)	(0, 3)	(1, 4)	(2, 5)	(3, 6)	(4, 0)	(5, 1)
(2, 3)	(3, 4)	(4, 5)	(5, 6)	(6, 0)	(0, 1)	(1, 2)
(3, 1)	(4, 2)	(5, 3)	(6, 4)	(0, 5)	(1, 6)	(2, 0)
(1, 5)	(2, 6)	(3, 0)	(4, 1)	(5, 2)	(6, 3)	(0, 4)
(5, 4)	(6, 5)	(0, 6)	(1, 0)	(2, 1)	(3, 2)	(4, 3)

(6.5.2) For $1 \le i \le 7$, let $\mathcal{R}_i = \{\{i, i + 1, i + 3\}, \{i + 2, i + 4, i + 5\}\}$ (mod 7). Then $(\cup_{1 \le i \le 7} \mathcal{R}_i) = \mathcal{B}_0 \cup \mathcal{B}_1$. Further, for each i, $(1 \le i \le 7)$, the pairs of points of Z_7 contained in the blocks of $\mathcal{A}_{i2}$ are precisely those contained in the triples of $\mathcal{R}_i$.

Now, suppose $v \equiv 1 \pmod 6$. What we will do is construct a 4-AD(1, 7v) given a 4-AD(1, v). We employ point set

$$X = Z_7 \times Z_v \cup \Omega,$$

where $\Omega = \{\infty_1, \infty_2, \infty_3, \infty_4\}$. The construction proceeds in several steps.

Step 1

For $1 \le i \le 7$, do the following. Take a 4-AD(1, v) on $\{i - 1\} \times Z_v \cup \Omega$. The v 3-GDD($1^{v-1}5^1$) are $(\{i - 1\} \times Z_v \cup \Omega, \mathcal{G}_j(i), \mathcal{A}_j(1, i))$ $(1 \le j \le v)$. $\mathcal{G}_j(i)$ consists of $(i - 1, j - 1) \cup \Omega$ and $(i - 1, k - 1)$, where $1 \le k \le v$, $k \ne j$. (There are $(v^2 + 7v - 8) / 6$ blocks in each $\mathcal{A}_j(1, i)$.) The block sets of the 2 3-GDD(1^v) are denoted by $\mathcal{B}_k(i)$ $(0 \le k < 2)$.

Step 2

For $1 \le i \le 7$ do the following. If $(a, b) \in D_i(2)$ and $\{x, a, b\} \in \mathcal{A}_{i1}$, take an LSDG($1^{v+1}v^1$) on $\{x\} \cup (\{a, b\} \times Z_v)$, with groups $\{x\}$, $\{(a, k)\}$ $(k \in Z_v)$, $\{(b, k): k \in Z_v\}$. (This large set exists by Lemma 2.2.2.) Name the v disjoint block sets $\mathcal{A}_j(a, b)$, $1 \le j \le$

v. Let $\mathcal{A}_j(2, i) = \cup_{(a,b) \in D_i(2)} \mathcal{A}_j(a, b)$, $1 \le j \le v$. (There are $3v(v + 1)$ blocks in each $\mathcal{A}_j(2, i)$, since a 3-GDD of type $1^{v+1}v^1$ has $v(v + 1) / 2$ blocks.)

Step 3

For $1 \le i \le 7$ do the following. If $R = \{a, b, c\} \in \mathcal{R}_i$, then take an LSDG($v^3$) on point set $R \times Z_v$, with groups $\{a\} \times Z_v$, $\{b\} \times Z_v$, $\{c\} \times Z_v$. We use Lemma 6.5.1. Let $\mathcal{B}_j(R)$ $(1 \le j \le v)$ be the v disjoint block sets. Let $\mathcal{P}_j(R) \subseteq \mathcal{B}_j(R)$ be a parallel class such that $\cup_{1 \le j \le v} \mathcal{P}_j(R)$ forms a block set of a 3-GDD of type v^3. If $\{x, a, b\}$, $\{y, b, c\}$, $\{z, c, a\}$ are in $\mathcal{A}_{i3}$, then let $\mathcal{C}_j(R)$ be equal to

$$\cup_{\{(a,r), (b,s), (c,t)\} \in \mathcal{P}_j(R)} \{ \{x, (a, r), (b, s)\}, \{y, (b, s), (c, t)\}, \{z, (c, t), (a, r)\} \}.$$

Since $\cup_{1 \le j \le v} \mathcal{P}_j(R)$ forms the block set of a 3-GDD of type v^3, it follows that $\mathcal{C}_j(R)$ $(1 \le j \le v)$ are disjoint. Let

$$\mathcal{A}_j(3, i) = \cup_{R \in \mathcal{R}_i} ((\mathcal{B}_j(R) \setminus \mathcal{P}_j(R) \cup \mathcal{C}_j(R)),$$

$1 \le j \le v$. (There are $2v^2 + 4v$ blocks in each $\mathcal{A}_j(3, i)$.)

Step 4

For $1 \le i \le 7$, do the following. If $A = \{a, b, c\} \in \mathcal{A}_{i3}$, then take an LSDG($v^3$) on point set $A \times Z_v$, with groups $\{a\} \times Z_v$, $\{b\} \times Z_v$, $\{c\} \times Z_v$. Name the v disjoint block sets $\mathcal{A}_j(A)$, $1 \le j \le v$. Let $\mathcal{A}_j(4, i) = \cup_{A \in \mathcal{A}_{i3}} \mathcal{A}_j(A)$. (There are $3v^2$ blocks in each $\mathcal{A}_j(4, i)$.)

Now we can present the construction of a 4-AD(1, 7v). First we present 7v 3-GDD($1^{7v-1}5^1$). For $1 \le i \le 7$ and $1 \le j \le v$, define

$$\mathcal{A}_j(i) = \mathcal{A}_j(1, i) \cup \mathcal{A}_j(2, i) \cup \mathcal{A}_j(3, i) \cup \mathcal{A}_j(4, i)$$

and

$$\mathcal{B}_0 = (\cup_{R \in \mathcal{R}'} \cup_{1 \le j \le v} \mathcal{P}_j(R)) \cup (\cup_{1 \le i \le 7} \mathcal{B}_0(i)),$$

where $\mathcal{R}' = \{\{i, i + 1, i + 3\}: 0 \le i \le 6\}$, and

$$\mathcal{B}_1 = (\cup_{R \in \mathcal{R}''} \cup_{1 \le j \le v} \mathcal{P}_j(R)) \cup (\cup_{1 \le i \le 7} \mathcal{B}_1(i)),$$

where $\mathcal{R}'' = \{\{i, i+1, i+3\}: 0 \le i \le 6\}$.

Then $(X, \mathcal{G}_j(i), \mathcal{A}_j(i))$ $(1 \le i \le 7, 1 \le j \le v)$ are 3-GDD($1^{7v-1}5^1$), where $\mathcal{G}_j(i)$ consists of $\{(i - 1, k - 1)\}$ $(1 \le i \le v, 1 \le k \le v, k \ne j)$ and $\{(i - 1, j - 1)\} \cup \Omega$. $(S, \mathcal{B}_0)$ and $(S, \mathcal{B}_0)$ are two 3-GDD(1^{7v}). Together they form a 4-AD(1, 7v). ♦

Therefore, we get the following.

Lemma 6.5.2 Suppose $v \equiv 1 \pmod 6$. If a 4-AD(1, v) exists, then a 4-AD(1, 7v) exists.

It would be nice if we had more 4-AD(1, v) with properties similar to those of 4-AD(1, 7), but we have not found any more examples yet.

In the above construction, if we did not define $\mathcal{B}_0$ and $\mathcal{B}_1$, we would only need an LSDP(v+4). Then we would end up with an LSDP(7v+4). This gives the following result.

Lemma 6.5.3 Suppose $v \equiv 1 \pmod 6$. If an LSDP(v+4) exists, then an LSDP(7v+4) exists.

6.6 Some small examples of 4-AD(1, v)

Here we construct a 4-AD(1, v) for v = 19, 25, 31, 43, 67.

Suppose $v \equiv 1 \pmod 6$ is a prime power. We take point set

$$X = GF(v) \cup \Omega,$$

where $\Omega = \{\infty_1, \infty_2, \infty_3, \infty_4\}$ and GF(v) is the finite field of order v. We will use the multiplicative structure of the field. Suppose ξ is a primitive element in GF(v). Let π be the permutation of X which multiplies each element of GF(v) by ξ but fixes ∞_1, ∞_2, ∞_3 and ∞_4.

We construct a 4-AD(1, v) on X. The v disjoint s-GDD($1^{v-1}5^1$) will be (X, $\mathcal{G}_x$, $\mathcal{A}_x$) ($1 \le x \le$ v). The idea is to construct $\mathcal{A}_1$, from which the others can be developed modulo v. The two 3-GDD(1^v) are (GF(v), $\mathcal{B}_0$) and (GF(v), $\mathcal{B}_1$) and have the following constructions.

Let $\mathcal{B}_0$ consist of blocks $\{1, \xi^{(v-1)/3}, \xi^{2(v-1)/3}\}\xi^k$, $0 \le k < (v - 1)/6$. Let $\mathcal{B}_0$ consist of blocks $\{1, \xi^{(v-1)/3}, \xi^{2(v-1)/3}\}\xi^k$, $(v - 1)/6 \le k < (v - 1)/3$. It is easy to check that (GF(v), $\mathcal{B}_0$) and (GF(v), $\mathcal{B}_1$) are disjoint 3-GDD(1^v).

We consider v a prime number. So, GF(v) = Z_v. In order to narrow down our search for $\mathcal{A}_1$, we assume the following properties hold:

(6.6.1) if $\{x, a, b\} \in \mathcal{A}_1$, then $\pi^2\{x, a, b\} \in \mathcal{A}_1$, where $x \in \{\infty_1, \infty_2, \infty_3, \infty_4\}$, $a, b \in Z_v$;

(6.6.2) if $\{a, b, c\} \in \mathcal{A}_1$, then $\pi\{a, b, c\} \in \mathcal{A}_1$, where $a, b, c \in Z_v$.

For a, b, c in Z_v, there are six i's such that $\pi^i\{a, b, c\}$ has the form $\{w, w + 1, w + u\}$. The set of six u's thus obtained is U(a, b, c). Two block sets developed from $\{a, b, c\}$ and $\{a', b', c'\}$ respectively (using π and developed modulo v), where $\{a, b, c, a', b', c'\} \subseteq Z_v$, are disjoint if and only if $U(a, b, c) \cap U(a', b', c') = \varnothing$ (Lemma 3.3.7--3.3.9). To check that $\mathcal{A}_1$ is a (2, 3)-packing, we simply check the exponential differences.

We succeed with this approach for v = 19 (Table 6.6.1), v = 43 (Table 6.6.2) and v = 67 (Table 6.6.3).

$\mathcal{A}_1$: ($\xi = 2$)		
blocks	developing by	U
$\{\infty_1, 1, \xi\}$, $\{\infty_2, \xi, \xi^2\}$ $\{\infty_3, 1, \xi^5\}$, $\{\infty_4, \xi, \xi^6\}$	π^2	
$\{0, 1, -1\}$	π (but orbit length 21)	2, 10, 18
$\{1, \xi^4, \xi^7\}$	π	3, 7, 9, 11, 13, 17
$\{1, \xi^6, \xi^8\}$	π	4, 5, 6, 14, 15, 16

Table 6.6.1

$\mathcal{A}_1$: ($\xi = 3$)		
blocks	developing by	U
$\{\infty_1, 1, \xi^5\}, \{\infty_2, \xi, \xi^6\}$ $\{\infty_3, 1, \xi^7\}, \{\infty_4, \xi, \xi^8\}$	π^2	
$\{0, 1, -1\}$	π (but orbit length 21)	2, 22, 42
$\{1, \xi^4, \xi^{12}\}$	π	3, 15, 21, 23, 29, 41
$\{1, \xi^2, \xi^{24}\}$	π	5, 12, 18, 26, 32, 39
$\{1, \xi^3, \xi^{19}\}$	π	4, 11, 14, 30, 33, 40
$\{1, \xi^6, \xi^{17}\}$	π	6, 8, 17, 27, 36, 38
$\{1, \xi^{13}, \xi^{28}\}$	π	9, 16, 20, 24, 28, 35
$\{1, \xi^1, \xi^{33}\}$	π	10, 13, 19, 25, 31, 34

Table 6.6.2

$\mathcal{A}_1$: ($\xi = 2$)		
blocks	developing by	U
$\{\infty_1, 1, \xi^{17}\}, \{\infty_2, \xi, \xi^{18}\}$ $\{\infty_3, 1, \xi^{19}\}, \{\infty_4, \xi, \xi^{20}\}$	π^2	
$\{0, 1, -1\}$	π (but orbit length 33)	2, 34, 66
$\{1, \xi^{14}, \xi^{38}\}$	π	3, 23, 33, 35, 45, 65
$\{1, \xi^{10}, \xi^{40}\}$	π	4, 17, 22, 46, 51, 64
$\{1, \xi^4, \xi^{22}\}$	π	6, 12, 28, 40, 56, 62
$\{1, \xi^6, \xi^{35}\}$	π	5, 18, 27, 41, 50, 63
$\{1, \xi^3, \xi^{23}\}$	π	7, 11, 20, 48, 57, 61
$\{1, \xi^5, \xi^{21}\}$	π	8, 19, 26, 42, 49, 60
$\{1, \xi^9, \xi^{34}\}$	π	9, 15, 25, 43, 53, 59
$\{1, \xi, \xi^{59}\}$	π	10, 16, 21, 47, 52, 58
$\{1, \xi^{12}, \xi^{27}\}$	π	13, 29, 31, 37, 39, 55
$\{1, \xi^2, \xi^{55}\}$	π	14, 24, 32, 36, 44, 54

Table 6.6.3

For v = 25, we use the finite field GF(25) of order 25, generated by the irreducible polynomial $x^2 + x + 2$ ($\xi = x$). Here we assume that:

(6.6.3) if $\{x, a, b\} \in \mathcal{A}_1$, then $\pi^8\{x, a, b\} \in \mathcal{A}_1$, where $x \in \{\infty_1, \infty_2, \infty_3, \infty_4\}$, a, b $\in$ GF(25);

(6.6.4) if $\{a, b, c\} \in \mathcal{A}_1$, then $\pi\{a, b, c\} \in \mathcal{A}_1$, where a, b, c $\in$ GF(25).

The result is listed in Table 6.6.4.

$\mathcal{A}_1$: $(x^2 + x + 2 = 0)$		
blocks	developing by	U
$\{\infty_1, x^8, x^{19}\}$, $\{\infty_1, x^4, x^{23}\}$ $\{\infty_1, x^{10}, x^{21}\}$, $\{\infty_1, x, x^6\}$	π^8	
$\{\infty_2, x^3, x^{22}\}$, $\{\infty_2, x^8, x^{21}\}$ $\{\infty_2, x^{17}, x^{12}\}$, $\{\infty_2, x^{10}, x^{23}\}$	π^8	
$\{\infty_3, x^7, x^{20}\}$, $\{\infty_3, x^{11}, x^{16}\}$ $\{\infty_3, x^9, x^{22}\}$, $\{\infty_3, x^{13}, x^{18}\}$	π^8	
$\{\infty_4, x^{10}, x^{15}\}$, $\{\infty_4, x^9, x^{20}\}$ $\{\infty_4, 1, x^5\}$, $\{\infty_4, x^{11}, x^{22}\}$	π^8	
$\{0, 1, x^{12}\}$	π(but orbit length 12)	x^6, x^{12}, x^{18}
$\{1, x^2, x^8\}$	π	$x^7, x^8, x^{11}, x^{13}, x^{16}, x^{17}$
$\{1, x, x^{10}\}$	π	$x^3, x^5, x^{10}, x^{14}, x^{19}, x^{21}$
$\{1, x^{17}, x^{20}\}$	π	$x, x^2, x^9, x^{15}, x^{22}, x^{23}$

Table 6.6.4

For v = 31, we need some small adjustments. Here we assume

(6.6.5) if $A \in \mathcal{A}_1$, then $\pi^2 A \in \mathcal{A}_1$.

For a, b, c in Z_v, there are three i's such that $\pi^{2i}\{a, b, c\}$ has the form $\{w, w + 1, w + v\}$. The set of three u's thus obtained is denoted by $U(\{a, b, c\})$. The result is listed in Table 6.6.5.

$\mathcal{A}_1$: ($\xi = 3$)		
blocks	developing by	U
$\{\infty_1, \xi, \xi^{18}\}$	π^2	
$\{\infty_2, 1, \xi^5\}$	π^2	
$\{\infty_3, 1, \xi^{15}\}$	π^2	
$\{\infty_4, \xi, \xi^{20}\}$	π^2	
$\{0, 1, \xi\}$	π^2	3, 11, 15
$\{\xi, \xi^3, \xi^9\}$	π^2	12, 18, 19
$\{1, \xi^2, \xi^6\}$	π^2	17, 21, 29
$\{1, \xi^8, \xi^{18}\}$	π^2	5, 23, 25
$\{1, \xi^{14}, \xi^3\}$	π^2	7, 9, 27
$\{\xi, \xi^5, \xi^6\}$	π^2	4, 8, 22
$\{\xi, \xi^{11}, \xi^{14}\}$	π^2	10, 24, 28
$\{\xi, \xi^{13}, \xi^{22}\}$	π^2	2, 16, 30
$\{\xi, \xi^8, \xi^{15}\}$	π^2	13, 14, 20

Table 6.6.5

6.7 Summary of the chapter

Applying Lemma 6.5.2 and using the results in Section 6.6 we have the following lemma.

Lemma 6.7.1 If $v = 7^i m$ where $i \geq 0$ and $m \in \{1, 7, 19, 25, 31, 43, 67\}$, then a 4-AD(1, v) exists.

The existence of a 4-AD(1, 13) is still unknown, though an LSDP(17) was presented in [2]. Using Lemma 6.4.3, we have the following.

Theorem 6.7.2 If $v = 7^i m$ where $i \geq 0$ and $m \in \{1, 7, 13, 19, 25, 31, 43, 67\}$, then an LSDP(7v+4) exists.

By Lemma 6.2.1, an LD(v) exists if $v \equiv 1 \pmod 6$. An LSDG($2^3 4^1$) is given by Example 4.3 in [2]. Using Lemma 6.4.1, we have the following (the necessary 4-AD(2, v) are given by Lemma 6.7.1 and Lemma 6.3.1.)

Theorem 6.7.3 If $v = 7^i m$ where $i \geq 0$ and $m \in \{1, 7, 19, 25, 31, 43, 67\}$, then an LSDG($2^3 v 4^1$) exists.

Chapter 7

Summarizing Results

7.1 Introduction

We will summarize all recursive constructions in section 7.2. We have mentioned in chapter 2 that, for $v \equiv 0$ or 2 (mod 6), an LSDG($2^{v/2}$) is an LSDP(v), for $v \equiv 4$ (mod 6), an LSDG($2^{(v-4)/2}4^1$) is an LSDP(v). Hence in the summary of section 7.2, we keep some recursive constructions in the form of disjoint 3-GDD.

7.2 Summary of recursive results

Construction I Suppose there exists an LSDG($t^u s^1$). Then an LSDG($((tw)^u(sw)^1$) exists for $w \geq 2$.

Construction II Suppose an LSDG(t^{u+2}) exists. Then an LSDG(t^{up+2}) exists, where p is a prime number and one of the following conditions is satisfied.

1) $p \equiv 7$ (mod 8);
2) $p \equiv 1$ (mod 8) and $p \leq 137$;
3) $u \geq 5$, $p \equiv 5$ (mod 8) and $p \leq 157$;
4) $p = 19$.

Construction III Suppose t is even and an LSDG(t^{u+2}) exists. Then an LSDG($t^{u(v-2)+2}$) exists, where $v \equiv 1$ or 3 (mod 6), $v > 1$.

Construction IV Suppose there exist an LSDG(t^{2u}) and an LSDG(t^6), where $u \neq 2, 6$. Then there exists an LSDG(t^{6u}).

Construction V Suppose there exist an LSDG($t^u s^1$) and an LSDG($t^3 s^1$), where $s \geq t$ and $u \neq 2, 6$. Then there exists an LSDG($t^{3u} s^1$).

Construction VI Suppose $u \geq 4$ is even and $t \in \{3, 6\}$. If an LSDG(t^{u-1}) exists, then there exists an LSDG(t^{2u-1}).

Construction VII Suppose $n \geq 3$. Suppose an n-AD(t, v) and an LD(v) exist. If there exists an LSDG($t^3(nt-2t)^1$), then there exists an LSDG($t^{3v}(nt-2t)^1$).

Construction VIII Suppose $v \equiv 1 \pmod 6$. If there exists an LSDP(v+4) = u, then an LSDP(7v+4) exists.

7.3 Summary of results on MP(v)

The following are values of MP(v) which reach the upper boundes of Theorem 1.2.1. If MP(v) reaches the upper bound of Theorem 1.2.1, then an LSDP(v) exists.

The following is a known result.

Theorem 7.3.1 For $v \equiv 1$ or 3 (mod 6), PM(v) = v - 2, except MP(7) = 3.

Now we prove the following.

Theorem 7.3.2 For $v \equiv 0$ or 2 (mod 6), PM(v) = v - 4, except possibly for $v \equiv 260$ or 516 (mod 768).

Proof. We show that an LSDG($2^{v/2}$) exists for $v \equiv 0$ or 2 (mod 6) except possibly for $v \equiv$ 260 or 516 (mod 768). Since LS(v/2) exists for $v > 14$ and $v \equiv 2$ or 6 (mod 12), an LSDG($2^{v/2}$) exists by Construction I. Since an LSDG(2^4) exists ([25]), an LSDG($t^{v/2}$) exists by Construction III, where $v \equiv 0$ or 8 (mod 24). Since an LSDG(2^6) exists ([2]), an LSDG($t^{v/2}$) exists by Construction III, where $v \equiv 12$ or 40 (mod 48). Since an LSDG(2^4) exists, by Construction V (take t = s = 2, u = 3), an LSDG(2^{10}) exists. Then by Construction III, an LSDG($2^{v/2}$) exists for $v \equiv 20$ or 84 (mod 96). Since an LSDG(2^6) exists, an LSDG(2^{18}) exists by Construction IV (take u = 3). Then by Construction III, an LSDG($2^{v/2}$) exists for $v \equiv 36$ or 164 (mod 192). Since an LSDG(2^{12}) exists, an LSDG(2^{34}) exists by Construction V (take t = s = 2, u = 11). Then by Construction III, an LSDG($2^{v/2}$) exists for $v \equiv 68$ or 324 (mod 384). This completes our proof. ♦

The following theorems is from Chapter 6 (Section 6.7, Theorem 6.7.2).

Theorem 7.3.3 For $v \equiv 5 \pmod 6$ and $v = 7^i m + 4$, where $i \geq 0$ and $m \in \{1, 7, 13, 19, 25, 31, 43, 67\}$, $PM(v) = v - 4$.

Theorem 7.3.4 For $v \equiv 4 \pmod 6$, if $v = 2.3^i + 4$ with $i > 0$ or if $v = 6.7^i m + 4$ with $i \geq 0$ and $m \in \{1, 7, 19, 25, 31, 43, 67\}$, then $PM(v) = v - 6$.

Proof. Since an $LSDG(2^3 4^1)$ exists (by [25]), an $LSDG(2^{3^i} 4^1)$ exists by Theorem 4.4.1 for $i > 0$. The rest of the theorem is from Theorem 6.7.3. ♦

References

[1] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, *A new table of constant weight codes*, IEEE Trans. Inform. Theory 36 (1990), pp. 1334-1380.

[2] D. Chen and D. R. Stinson, *Recent results on combinatorial constructions for threshold schemes*, Australasian J. of Combinatorics 1 (1990), pp.29-48.

[3] D. Chen and D. R. Stinson, *On the construction of large sets of disjoint group-divisible designs*, Ars Combinatoria 35(1993), pp. 103-115.

[4] D. Chen, R. G. Stanton, D. R. Stinson, *Disjoint packings on 6k+5 points*, Utilitas Mathematica 40 (1991), pp. 129-138.

[5] D. Chen, C. C. Lindner and D. R. Stinson, *Further results on large sets of disjoint group-divisible designs*, Discrete Math., 110(1992), pp. 35-42.

[6] C. J. Colbourn, A. Rosa and D. R. Stinson, *Pairwise balanced designs with block size three and four*, Canad. J. Math. 43(1991), pp. 673-704.

[7] C. J. Colbourn, D. G. Hoffman and R. Rees, *A new class of group divisible designs with block size three*, J. Comb. Theory A 45(1992), pp. 73-89.

[8] R. H. F. Denniston, *Some packings with Steiner triple systems*, Discrete Math. 9(1974), pp. 213-227.

[9] T. Etzion, *Optimal partitions for triples*, J. Comb. Theory A 59(1992) pp. 161-176.

[10] T. Etzion, *Partitions of triples into optimal packings*, J. Comb. Theory A 59(1992) pp. 269-284.

[11] C.-M. K. Fu, *The intersection problem for pentagon systems*, Ph.D. Thesis, Auburn University, 1987.

[12] H. Hanani, *On quadruple systems*, Canadian J. Math. 12(1960), pp. 131-140.

[13] A. Hartman, W. H. Mills, and R. C. Mullin, *Covering triples by quadruples: An asymptotic solution*, J. Comb. Theory (A) 41(1986), pp. 117-138.

[14] Kang Qingde, *A recurrence construction of LD-design*, Acta Mathematicae Applicatae Sinica, Vol. 10, No. 4 (1987), pp. 481-490.

[15] Kang Qingde, *The construction of large sets of disjoint Mendelsohn triple systems of order* 2^n+2, Discrete Math. 90(1991), pp. 199-205.

[16] Kang Qingde and Chang Yanxun, *Symmetric Mendelsohn triple systems and large sets of disjoint Mendelsohn triple systems*, Lecture Notes in Pure and Applied Math. 126(1990), pp. 69-78.

[17] Kang Qingde and Chang Yanxun, *Further results about large sets of disjoint Mendelsohn triple systems*, Chinese Science Bulletin 37(1992), pp.90-91.

[18] C. C. Lindner, *On the number of disjoint Mendelsohn triple systems*, J. Comb. Theory (A) 30 (1981), pp. 326-330.

[19] C. C. Lindner and A. P. Street, *Construction of large sets of pairwise disjoint transitive triple systems*, Europ. J. Comb. 4 (1983), pp. 335-346.

[20] J. X. Lu, *On large sets of disjoint Steiner triple systems* I, II, and III, J. Comb. Theory (A) 34(1983), pp. 140-146, 147-155, and 156-182.

[21] J. X. Lu, *On large sets of disjoint Steiner triple systems* IV, V, and VI, J. Comb. Theory (A) 37(1984), pp. 136-163, 164-188, and 189-192.

[22] W. H. Mills, *On the covering of triples by quadruples*, Congressus Numerantium X, pp. 563-581.

[23] A. Rosa, *A theorem on the maximum number of disjoint Steiner triple systems*, J. Comb. Theory (A) 18(1975), pp. 305-312.

[24] H. J. Ryser, *Combinatorial Mathematics*, published by The Mathematical Association of America, 1963.

[25] P. J. Schellenberg and D. R. Stinson, *Threshold schemes from combinatorial designs*, J. Comb. Math. and Comb. Comput. 5(1989), pp. 143-160.

[26] J. Schonheim, *On maximal systems of k-tuples*, Studia Sci. Math. Hung. 1 (1966), pp. 363-368.

[27] J. Spencer, *Maximal consistent families of triples*, J. Comb. Theory 5 (1968), pp. 1-8.

[28] D. R. Stinson and S. A. Vanstone, *A combinatorial approach to threshold schemes*, SIAM J. on Discrete Math. 1(1988), pp. 230-236.

[29] L. Teirlinck and C. C. Lindner, *The construction of large sets of idempotent quasigroups*, European J. Comb. 9(1988), pp. 83-89.

[30] L. Teirlinck, *A completion of Lu's determination of the spectrum for large sets of disjoint Steiner triple systems*, J. Comb. Theory (A) 57(1991), pp. 302-305.

[31] L. Teirlinck, *Large sets of disjoint designs and related structures*, in "Contemporary Design Theory : A Collection of Surveys", Wiley, New York, 1992, pp. 561-592.

[32] L. Teirlinck, *On large sets of disjoint quadruple systems*, Ars Combinatotia 17(1984), pp. 173-176.

[33] L. Teirlinck, *Non-trivial t-designs without repeated blocks exist for all t*, Discrete Math. 65(1987), pp. 301-311.

[34] L. Teirlinck, *Large sets with holes*, J. Combin. Designs, 1(1993), pp.69-94.

[35] C. L. M. Van Pul and T. Etzion, *New lower bounds for constant weight codes*, IEEE Trans. Inform. Theory 35 (1989), pp. 1324-1329.

[36] R. M. Wilson, *Some partitions of all triples into Steiner triple systems*, Lecture Notes in Math. 411, Springer-Verlag, New York, 1974, pp. 267-277.

Appendix I (for Chapter 3)

To construct a satisfactory STS(p+2) $(X, \mathcal{A})$ we construct $\mathcal{R}$. The following tables list $\mathcal{R}$ whose elements are in exponential form (except ϕ, which is the zero of Z_p), i.e., triple {x, y, z} is actually $\{\xi^x, \xi^y, \xi^z\}$ in $\mathcal{R}$. To make checking easy, we also list the exponential differences and the corresponding U-set of each triple. ξ is a primitive element of the field Z_p.

p = 41, ξ = 6, h = 4

{x, y, z}	exponential difference	U(ξ^x, ξ^y, ξ^z)
ϕ, 1, -1	dif : 20	U : 2 40 21
0, 1, 7	dif : 1, 6, 7	U : 3 28 22 39 20 14
0, 2, 15	dif : 2, 13, 15	U : 4 38 27 15 11 31
0, 5, 23	dif : 5, 17, 18	U : 5 32 33 9 10 37
0, 3, 31	dif : 3, 9, 12	U : 6 35 34 36 8 7
0, 8, 29	dif : 8, 11, 19	U : 12 18 26 30 24 16
0, 10, 24	dif : 10, 14, 16	U : 13 19 23 25 29 17

p = 73, ξ = 5, h = 4

{x, y, z}	exponential difference	U(ξ^x, ξ^y, ξ^z)
ϕ, 1, -1	dif : 36	U : 2 72 37
0, 24, 48	dif : 24	U : 9
0, 1, 27	dif : 1, 26, 27	U : 3 49 25 38 71 36
0, 2, 8	dif : 2, 6, 8	U : 4 70 24 55 50 19
0, 3, 32	dif : 3, 29, 32	U : 5 69 18 44 56 30
0, 5, 16	dif : 5, 11, 16	U : 6 68 45 29 13 61
0, 10, 54	dif : 10, 18, 28	U : 7 62 53 67 21 12
0, 7, 21	dif : 7, 14, 21	U : 8 22 52 66 64 10
0, 15, 49	dif : 15, 23, 34	U : 11 20 63 51 54 23
0, 12, 25	dif : 12, 13, 25	U : 14 47 60 28 27 46
0, 9, 39	dif : 9, 30, 33	U : 15 59 26 39 48 35
0, 17, 52	dif : 17, 20, 35	U : 16 42 40 32 34 58
0, 19, 50	dif : 19, 22, 31	U : 17 33 43 31 41 57

p = 89, ξ = 3, h = 4

{x, y, z}	exponential difference	U(ξ^x, ξ^y, ξ^z)
ϕ, 1, -1	dif : 44	U : 2 88 45
0, 1, 32	dif : 1, 31, 32	U : 3 60 46 87 44 30

0, 2, 13	dif : 2, 11, 13	U : 4 86 59 67 31 23
0, 3, 10	dif : 3, 7, 10	U : 5 18 85 22 72 68
0, 5, 17	dif : 5, 12, 17	U : 6 84 71 75 19 15
0, 6, 25	dif : 6, 19, 25	U : 7 83 74 39 16 51
0, 8, 72	dif : 8, 16, 24	U : 8 52 78 12 38 82
0, 9, 47	dif : 9, 38, 41	U : 9 80 79 10 11 81
0, 21, 55	dif : 21, 33, 34	U : 13 48 42 53 77 37
0, 22, 45	dif : 22, 23, 43	U : 14 70 20 49 76 41
0, 15, 52	dif : 15, 36, 37	U : 17 21 73 50 69 40
0, 18, 48	dif : 18, 30, 40	U : 24 66 58 64 32 26
0, 14, 42	dif : 14, 28, 42	U : 25 65 63 57 27 33
0, 20, 59	dif : 20, 29, 39	U : 28 35 55 34 62 56
0, 26, 53	dif : 26, 27, 35	U : 29 47 43 36 54 61

$p = 97, \xi = 5, h = 16$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 48	U : 2 96 49
0, 32, 64	dif : 32	U : 36
0, 1, 25	dif : 1, 24, 25	U : 3 65 95 48 33 50
0, 2, 31	dif : 2, 29, 31	U : 4 73 25 66 94 32
0, 3, 39	dif : 3, 36, 39	U : 5 74 59 39 24 93
0, 4, 23	dif : 4, 19, 23	U : 6 92 58 81 40 17
0, 5, 54	dif : 5, 42, 47	U : 7 84 82 91 16 14
0, 6, 44	dif : 6, 38, 44	U : 8 15 83 90 85 13
0, 10, 66	dif : 10, 30, 40	U : 9 89 12 54 86 44
0, 7, 27	dif : 7, 20, 27	U : 10 68 30 55 88 43
0, 18, 53	dif : 18, 35, 43	U : 11 87 69 45 29 53
0, 9, 59	dif : 9, 37, 46	U : 18 71 57 80 41 27
0, 15, 41	dif : 15, 26, 41	U : 19 46 79 70 52 28
0, 11, 79	dif : 11, 17, 28	U : 20 64 51 78 47 34
0, 8, 82	dif : 8, 14, 22	U : 21 77 63 37 35 61
0, 13, 75	dif : 13, 21, 34	U : 22 38 75 23 60 76
0, 12, 63	dif : 12, 33, 45	U : 26 67 42 72 56 31

$p = 113, \xi = 3, h = 8$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 56	U : 2 112 57
0, 1, 7	dif : 1, 6, 7	U : 3 76 58 38 56 111
0, 2, 26	dif : 2, 24, 26	U : 4 110 75 39 29 85
0, 3, 14	dif : 3, 11, 14	U : 5 68 109 28 46 86
0, 4, 46	dif : 4, 42, 46	U : 6 19 95 69 108 45
0, 5, 33	dif : 5, 28, 33	U : 7 97 17 20107 94
0, 9, 49	dif : 9, 40, 49	U : 8 99 106 16 15 98
0, 10, 35	dif : 10, 25, 35	U : 9 105 100 26 14 88
0, 12, 34	dif : 12, 22, 34	U : 10 104 89 80 25 34

0, 16, 61	dif : 16, 45, 51	U : 11 42 72 35 79 103
0, 19, 83	dif : 19, 29, 48	U : 12 73 48 102 66 41
0, 15, 47	dif : 15, 32, 47	U : 13 101 47 87 67 27
0, 23, 60	dif : 23, 37, 52	U : 18 96 93 70 21 44
0, 13, 68	dif : 13, 44, 55	U : 22 36 92 43 78 71
0, 27, 58	dif : 27, 31, 54	U : 23 91 77 55 37 59
0, 18, 38	dif : 18, 20, 38	U : 24 81 60 90 54 33
0, 21, 71	dif : 21, 41, 50	U : 30 65 74 84 49 40
0, 30, 73	dif : 30, 39, 43	U : 31 62 83 64 52 50
0, 17, 53	dif : 17, 36, 53	U : 32 63 61 82 53 51

$p = 137, \xi = 3, h = 4$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 68	U : 2 136 69
0, 1, 20	dif : 1, 19, 20	U : 3 92 70 135 68 46
0, 2, 42	dif : 2, 40, 42	U : 4 47 103 35 91 134
0, 3, 44	dif : 3, 41, 44	U : 5 133 104 83 34 55
0, 5, 17	dif : 5, 12, 17	U : 6 115 82 132 56 23
0, 6, 28	dif : 6, 22, 28	U : 7 40 98 24 114 131
0, 7, 86	dif : 7, 50, 57	U : 8 99 120 18 39130
0, 8, 98	dif : 8, 38, 46	U : 9 129 17 61 121 77
0, 9, 35	dif : 9, 26, 35	U : 10 62 76 128 96 42
0, 10, 21	dif : 10, 11, 21	U : 11 25 127 41 113 97
0, 14, 76	dif : 14, 60, 62	U : 12 80 126 112 58 26
0, 15, 67	dif : 15, 52, 67	U : 13 116 22 81 125 57
0, 29,104	dif : 29, 32, 61	U : 14 117 89 124 49 21
0, 18, 63	dif : 18, 45, 63	U : 15 64 123 88 74 50
0, 30, 77	dif : 30, 47, 59	U : 16 78 73 122 65 60
0, 23, 93	dif : 23, 43, 66	U : 19 100 101 37 38 119
0, 13, 49	dif : 13, 36, 49	U : 20 48 118 36 90 102
0, 27, 80	dif : 27, 53, 56	U : 27 66 111 79 72 59
0, 24, 88	dif : 24, 48, 64	U : 28 67 71 110 93 45
0, 34, 71	dif : 34, 37, 65	U : 29 109 94 86 44 52
0, 25,103	dif : 25, 33, 58	U : 30 32 106 53 108 85
0, 31, 85	dif : 31, 51, 54	U : 31 54 84 33 105 107
0, 16, 97	dif : 16, 39, 55	U : 43 51 95 75 87 63

Appendix II (for Chapter 3)

The following tables list $\mathcal{R}$. All elements are in exponential form (except ϕ, which is the zero of Z_p), i.e., triple {x, y, z} is actually $\{\xi^x,\xi^y,\xi^z\}$ in $\mathcal{R}$. To make checking easy, we also list the exponential differences and the corresponding U-set of each triple. ξ is a primitive element of the field Z_p.

$p = 5, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 2	U : 2, 3, 4

$p = 13, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 6	U : 2, 12, 7
0, 4, 8	dif : 4	U : 4
0, 2, 5	dif : 2, 3, 5	U : 3, 11, 8, 6, 5, 9

$p = 37, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 18	U : 2, 36, 19
0, 12, 24	dif : 12	U : 27
0, 2, 5	dif : 2, 3, 5	U : 3, 35, 18, 25, 20, 13
0, 7, 23	dif : 7, 13, 16	U : 4, 28, 10, 26, 34, 12
0, 9, 26	dif : 9, 10, 17	U : 5, 15, 33, 9, 23, 29
0, 6, 14	dif : 6, 8, 14	U : 6, 31, 7, 16, 32, 22
0, 4, 25	dif : 4, 11, 15	U : 8, 30, 21, 24, 17, 14

$p = 53, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 26	U : 2, 52, 27
0, 2, 5	dif : 2, 3, 5	U : 3, 36, 28, 51, 26, 18
0, 4, 31	dif : 4, 21, 25	U : 4, 19, 35, 50, 40, 14
0, 8, 40	dif : 8, 12, 20	U : 5, 41, 32, 22, 13, 49
0, 14, 30	dif : 14, 16, 22	U : 6, 9, 48, 21, 45, 33
0, 9, 24	dif : 9, 15, 24	U : 7, 47, 44, 16, 10, 38
0, 6, 39	dif : 6, 13, 19	U : 8, 39, 34, 20, 15, 46

0, 7, 17	dif : 7, 10, 17	U : 11, 43, 37, 29, 17, 25
0, 11, 34	dif : 11, 18, 23	U : 12, 42, 24, 31, 30, 23

$p = 61, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 30	U : 2, 60, 31
0, 20, 40	dif : 20	U : 48
0, 2, 6	dif : 2, 4, 6	U : 3, 32, 41, 21, 30, 59
0, 3, 13	dif : 3, 10, 13	U : 4, 46, 16, 42, 58, 20
0, 5, 27	dif : 5, 22, 27	U : 5, 47, 49, 13, 15, 57
0, 12, 43	dif : 12, 17, 29	U : 6, 51, 11, 50, 56, 12
0, 8, 32	dif : 8, 24, 28	U : 7, 55, 10, 35, 52, 27
0, 18, 41	dif : 18, 19, 23	U : 8, 23, 54, 26, 39, 36
0, 9, 44	dif : 9, 16, 25	U : 9, 34, 53, 38, 28, 24
0, 7, 21	dif : 7, 14, 21	U : 17, 44, 43, 45, 19, 18
0, 11, 26	dif : 11, 15, 26	U : 22, 40, 29, 25, 33, 37

$p = 101, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 50	U : 2, 100, 51
0, 2, 12	dif : 2, 10, 12	U : 3, 68, 52, 99, 50, 34
0, 3, 11	dif : 3, 8, 11	U : 4, 76, 26, 35, 98, 67
0, 4, 61	dif : 4, 39, 43	U : 5, 97, 77, 25, 21, 81
0, 5, 25	dif : 5, 20, 25	U : 6, 85, 82, 17, 20, 96
0, 6, 37	dif : 6, 31, 37	U : 7, 73, 29, 18, 84, 95
0, 7, 28	dif : 7, 21, 28	U : 8, 38, 64, 30, 94, 72
0, 9, 55	dif : 9, 45, 46	U : 9, 45, 57, 39, 93, 63
0, 13, 65	dif : 13, 35, 48	U : 10, 46, 56, 92, 91, 11
0, 17, 68	dif : 17, 32, 49	U : 12, 47, 59, 43, 55, 90
0, 14, 81	dif : 14, 19, 33	U : 13, 60, 70, 32, 42, 89
0, 15, 73	dif : 15, 27, 42	U : 14, 88, 31, 65, 71, 37
0, 22, 62	dif : 22, 38, 40	U : 15, 75, 66, 27, 36, 87
0, 24, 71	dif : 24, 29, 47	U : 16, 83, 74, 86, 28, 19
0, 26, 70	dif : 26, 30, 44	U : 22, 80, 24, 23, 78, 79
0, 16, 82	dif : 16, 18, 34	U : 33, 69, 61, 53, 41, 49
0, 23, 59	dif : 23, 36, 41	U : 40, 62, 44, 48, 58, 54

$p = 109, \xi = 6, h = 57$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 54	U : 2, 108, 55
0, 36, 72	dif : 36	U : 64

0, 1, 11	dif : 1, 10, 11	U : 3, 73, 37, 56,107, 54
0, 2, 5	dif : 2, 3, 5	U : 4, 82, 28, 74,106, 36
0, 4, 41	dif : 4, 37, 41	U : 5, 22, 88, 83,105, 27
0, 6, 65	dif : 6, 43, 49	U : 6, 23, 87,104, 91, 19
0, 7, 38	dif : 7, 31, 38	U : 7,103, 92, 32, 18, 78
0, 8, 21	dif : 8, 13, 21	U : 8,102, 31, 41, 79, 69
0, 9, 34	dif : 9, 25, 34	U : 9, 97,101, 68, 13, 42
0, 12, 85	dif : 12, 23, 35	U : 10, 99, 98, 11, 12,100
0, 14, 80	dif : 14, 28, 42	U : 14, 96, 67, 71, 43, 39
0, 22, 61	dif : 22, 39, 47	U : 15, 95, 70, 80, 40, 30
0, 24, 51	dif : 24, 27, 51	U : 16, 81, 35, 94, 75, 29
0, 16, 56	dif : 16, 40, 52	U : 17, 77, 33, 76, 93, 34
0, 19, 48	dif : 19, 29, 48	U : 20, 90, 86, 60, 24, 50
0, 15, 78	dif : 15, 30, 45	U : 21, 26, 89, 49, 84, 61
0, 20, 75	dif : 20, 33, 53	U : 25, 48, 62, 51, 85, 59
0, 18, 64	dif : 18, 44, 46	U : 38, 57, 66, 44, 53, 72
0, 26, 58	dif : 26, 32, 50	U : 45, 63, 47, 58, 65, 52

$p = 149, \xi = 2, h = 1$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 74	U : 2, 148, 75
0, 2, 30	dif : 2, 28, 30	U : 3,147, 74, 50, 76,100
0, 3, 32	dif : 3, 29, 32	U : 4,146, 99,112, 51, 38
0, 4, 23	dif : 4, 19, 23	U : 5,120,113,145, 37, 30
0, 5, 85	dif : 5, 63, 68	U : 6, 25,144,119,125, 31
0, 6, 65	dif : 6, 59, 65	U : 7, 86, 64, 26,124,143
0, 7, 38	dif : 7, 31, 38	U : 8, 94, 85,142, 65, 56
0, 8, 25	dif : 8, 17, 25	U : 9,116, 34, 57,141, 93
0, 9, 81	dif : 9, 67, 72	U : 10,140, 33, 15,117,135
0, 10, 55	dif : 10, 45, 55	U : 11,139,134,122, 16, 28
0, 11, 50	dif : 11, 39, 50	U : 12,138, 27, 87,123, 63
0, 12, 27	dif : 12, 15, 27	U : 13, 23,127, 88,137, 62
0, 13, 71	dif : 13, 58, 71	U : 14,136,126,118, 24, 32
0, 18, 84	dif : 18, 64, 66	U : 17, 36,121,133,114, 29
0, 14,114	dif : 14, 34, 48	U : 18,132,115, 92, 35, 58
0, 21, 94	dif : 21, 54, 73	U : 19,102, 48, 59,131, 91
0, 16,115	dif : 16, 33, 49	U : 20,103, 68,130, 82, 47
0, 41, 92	dif : 41, 51, 56	U : 21, 71,129, 67, 79, 83
0, 40,102	dif : 40, 46, 62	U : 22,128, 78, 61, 72, 89
0, 35,105	dif : 35, 43, 70	U : 39,111, 98,107, 52, 43
0, 26, 95	dif : 26, 53, 69	U : 40, 41,110, 42,109,108
0, 44, 91	dif : 44, 47, 57	U : 44, 53, 97,106,105, 45
0, 24, 61	dif : 24, 37, 61	U : 46, 69, 81, 54, 96,104
0, 20,126	dif : 20, 22, 42	U : 49,101, 90, 77, 60, 73
0, 36, 88	dif : 36, 52, 60	U : 55, 84, 66, 70, 95, 80

$p = 157, \xi = 5, h = 141$

{x, y, z}	exponential difference	$U(\xi^x, \xi^y, \xi^z)$
ϕ, 1, -1	dif : 78	U : 2, 156, 79
0, 52, 104	dif : 52	U : 13
0, 1, 26	dif : 1, 25, 26	U : 3,105,155, 78, 53, 80
0, 2, 69	dif : 2, 67, 69	U : 4,154,106, 52, 40,118
0, 3, 38	dif : 3, 35, 38	U : 5, 63, 95,119,153, 39
0, 4, 45	dif : 4, 41, 45	U : 6, 64, 94,152,131, 27
0, 5, 19	dif : 5, 14, 19	U : 7,132,113, 45, 26,151
0, 6, 99	dif : 6, 57, 63	U : 8, 99,112,150, 59, 46
0, 7, 20	dif : 7, 13, 20	U : 9, 35,149, 98,123, 60
0, 8, 80	dif : 8, 72, 76	U : 10, 48,122,148,110, 36
0, 9, 21	dif : 9, 12, 21	U : 11,111,100, 58, 47,147
0, 10, 40	dif : 10, 30, 40	U : 12,101, 57,146,144, 14
0, 11, 29	dif : 11, 18, 29	U : 15, 21,137,102,143, 56
0, 15, 64	dif : 15, 49, 64	U : 16, 50,136,142,108, 22
0, 16, 48	dif : 16, 32, 48	U : 17,141,109,121, 49, 37
0, 17, 98	dif : 17, 58, 75	U : 18, 62, 96, 38,120,140
0, 47,100	dif : 47, 53, 56	U : 19, 97, 61,139,124, 34
0, 34, 85	dif : 34, 51, 71	U : 20,138,125,103, 33, 55
0, 22, 95	dif : 22, 61, 73	U : 23,135,107, 41, 51,117
0, 33, 77	dif : 33, 44, 77	U : 24, 86,116,134, 72, 42
0, 36,101	dif : 36, 55, 65	U : 25, 44,114, 73,133, 85
0, 24, 66	dif : 24, 42, 66	U : 28, 65, 93,130,129, 29
0, 27, 97	dif : 27, 59, 70	U : 30,128, 92, 69, 66, 89
0, 31,119	dif : 31, 37, 68	U : 31,127, 68, 76, 90, 82
0, 46,106	dif : 46, 50, 60	U : 32, 54,126, 81,104, 77
0, 28,102	dif : 28, 54, 74	U : 43, 84, 74, 87,115, 71
0, 23,117	dif : 23, 39, 62	U : 67, 75, 83, 70, 91, 88